UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO-CAMPUS SUR

CARRERA DE INGENIERÍA EN SISTEMAS

“DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL SEGURA PARA LAS OFICINAS DE CAMINOSCA S.A BASADO EN PLATAFORMA GNU/LINUX”

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

DEISY PATRICIA CANSINO HENAO

DIRECTOR: ING. RAFAEL JAYA.

QUITO DICIEMBRE DEL 2012

DECLARACIÓN

Yo, Deisy Patricia Cansino Henao, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad intelectual, por su reglamento y por la normatividad vigente.

Deisy Patricia Cansino Henao

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Deisy Patricia Cansino Henao, bajo mi dirección.

Ing. Rafael Jaya

Director de Proyecto de Tesis

DEDICATORIA

El presente trabajo está dedicado a Dios, por darme la oportunidad de vivir y darme una hermosa familia.

A mis queridos padres por sus consejos y el apoyo incondicional que me han brindado a lo largo de mi carrera, a mi padre por brindarme los recursos necesarios, a mi madre por hacer de mi una mejor persona con sus consejos y sus ánimos, a mis hermanos por estar siempre presentes gracias por brindarme su confianza y apoyo.

Gracias por ayudarme a cumplir mis objetivos como persona y estudiante.

Deisy Cansino

CONTENIDO

Índice de figuras

Índice de tablas

PRESENTACIÓN

A lo largo del documento se da a conocer el hardware y software requerido, sus ventajas y limitaciones, para este tipo de conexiones se debe tener conocimiento del manejo de GNU/Linux y Openvpn, para su correcto funcionamiento, por lo cual, en este proyecto de tesis se explica paso a paso la configuración de cada uno de los software que se va a utilizar para la correcta conexión, tanto para el servidor-Linux como para el cliente-Windows Xp, se verificará el envío y recepción de información.

En el capítulo I, se presenta los problemas que se encontraron en la empresa, actualmente, en la empresa tiene comunicación entre las computadoras que se encuentran en diferentes redes por medio del correo y FTP en el cual existe varias dificultades al momento de enviar y recibir información, motivo por el cual la implementación de una red privada virtual es una propuesta para dar solución a este problema los objetivos a cumplirse y la metodología que se utilizará para realizar la conexión, obteniendo de esta manera seguridad y confiabilidad al transmitir los datos de un lugar a otro, mediante la utilización de protocolos de autenticación, y algoritmos de encriptamiento, los mismos que vienen incluidos dentro del sistemas operativo GNY/LINUX.

En el capítulo II, se revisará varios conceptos de hardware y software, características, tipos, beneficios y el diseño de una VPN para la conexión que se realizará.

En el capítulo III, se analizará la situación actual de la empresa, las soluciones y descripción de las herramientas de trabajo, y la descripción de los sistemas operativos que se utilizará para la realización del proyecto de tesis.

En el capítulo IV, se analiza los requerimientos necesarios para la configuración y conexión de la VPN tanto del servidor como del cliente. Se detalla el diseño de la VPN que se realizará, la instalación de OpenVPN, en el servidor como en el cliente.

En el capítulo V, se tiene las pruebas de conexión realizadas, entre el servidor-cliente, el cliente con la dirección creado por Openvpn para el túnel por donde pasa la información cifrada hacia el servidor, y finalmente se analiza el Ancho de Banda.

Se conocerá las conclusiones y recomendaciones a las cuales se llego por medio de la realización de este proyecto.

CAPÍTULO 1

INTRODUCCIÓN

1.1 ANTECEDENTES

En el presente trabajo, se analiza el diseño y la implementación de una VPN (Red Privada Virtual), para la interconexión desde las oficinas matriz de Caminosca S.A hacia la oficina sucursal y la conexión de usuarios remotos.

Se analizan todas las necesidades y problemas que la empresa requiere para que la comunicación sea segura y confiable, como solución se presentará propuestas de VPN'S a través de internet.

1.2 AMBITO

La empresa Caminosca S.A. se encuentra ubicada en el Norte de la ciudad de Quito, la empresa es una consultora de proyectos cuya misión es "Hacer ingeniería para crear obras exitosas", la cual cuenta con oficinas dentro y fuera de ciudad.

Los diferentes proyectos que la empresa realiza necesitan comunicarse diariamente con la oficina matriz para intercambiar información y los avances de los proyectos que se están realizando.

Para la empresa es muy importante mantenerse en contacto directo con sus clientes y mantener la información actualizada esto lo hacen por medio del correo electrónico, por HTP y por medios físicos como cd's, usb, memorias externas.

1.3 PLANTEAMIENTO DEL PROBLEMA

Caminosca es una empresa consultora de ingeniería, su misión es ayudar a sus clientes a lograr eficacia en sus proyectos, la empresa tiene varios campamentos de trabajo a nivel nacional y brinda servicios también a nivel internacional, por tal

motivo la empresa tiene gran cantidad e información que recibe y envía de sus clientes.

Toda la información que se procesa en las oficinas se almacena en lo servidores**,** de esta manera se mantiene la información centralizada.

Caminosca cuenta con una red de más de 150 equipos, cuyos usuarios acceden a la información almacenada en los servidores a través del protocolo SMB. Para mantener la privacidad de la información, cada usuarios tiene acceso únicamente a la información necesaria para realizar su trabajo, de acuerdo con un esquema de asignación de permisos desarrollado por Caminosca.

El problema real, se presenta con los usuarios externos, ya que las únicas dos vías que se tienen para que ellos tengan acceso a esta información es mediante correo electrónico o a través del un FTP propio de Caminosca.

El correo electrónico permite la transferencia de archivos hasta de 5MB, el FTP es un espacio abierto se puede transferir archivos de cualquier tamaño.

En el FTP, se puede transferir información ilimitada, el problema es que al momento de cargar y descargar información tarda mucho tiempo, por saturación del canal.

Con la implementación de la VPN no se busca mejorar el ancho de banda, si no la seguridad de la información, ya que la comunicación entre las oficinas de Caminosca y el campamento es información muy importante y confidencial para la empresa.

Cabe aclarar que la VPN va hacer utilizada para un campamento específicamente, ya que con este campamento es donde se presenta el mayor problema por la cantidad de información que se maneja, para el resto de campamentos se mantendrá el uso del correo electrónico, SMB y el FTP.

Ante los antecedentes mencionados, la empresa cree conveniente utilizar un servicio privado como una VPN (Virtual Private Network), por tanto, es propicia la investigación de que tan conveniente sería utilizar este servicio.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Implementar VPN basado en la plataforma GNU/Linux para tener una conexión rápida y segura, sin filtraciones y perdida de información entre la matriz de Caminosca S.A. y cualquier usuario que se encuentre fuera de su red local y cuente con una conexión a Internet.

1.4.2 OBJETIVOS ESPECÍFICOS

- Investigar que tecnologías se pueden usar y cuales soportan a la VPN.
- Lograr una buena conexión por medio de VPN bajo la plataforma de GNU/Linux, para mejorar la transmisión de información, sin que haya duplicidad de datos y pérdida de tiempo al momento de la transmisión.
- Acceder a los equipos de la empresa por medio de una conexión remota y trabajar desde cualquier equipo que tenga una conexión a Internet y así facilitar el trabajo.
- Implementar todos los niveles de seguridad necesaria para garantizar la fiabilidad de la información y evitar la apropiación de esta información por personas ajenas a la empresa.

1.5 JUSTIFICACIÓN DEL PROBLEMA

1.5.1 JUSTIFICACIÓN TEÓRICA

En la actualidad con el uso del Internet en el mundo de los negocios, se ha iniciado un proceso de transformación radical en la forma de hacer negocios, incluso de crear y desarrollar las empresas.

Internet es una excelente herramienta para mejorar la operativa de todo negocio, crear nuevos productos o servicios, abrir nuevos mercados y sobre todo, mejorar los procesos de comunicación empresarial. Por medio de la tecnología del Internet que hoy en día es tan necesaria ya es posible crear desde una empresa

matriz, y poder conectarse con equipos que se encuentran fuera de la red, y trabajar de manera remota con otros equipos.

Por medio del internet se puede tener gran comunicación con todo el mundo y para la empresa Caminosca S.A. esto es muy importante, la empresa se comunica con varios usuarios de varios lugares del País, por tal motivo se vio la necesidad de implementar una conexión VPN con GNU/Linux a través del internet para tener una mayor seguridad en la transmisión de datos.

Se utilizará GNU/Linux por la buena seguridad del sistema, GNU/Linux y la comunidad del software libre son muy sensibles a asegurarse de que los arreglos de problemas de seguridad entren en la distribución rápidamente. Normalmente, los paquetes arreglados se hacen disponibles a los pocos días.

La clave de sesión es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave de sesión y acto seguido usa la clave de sesión para descifrar el mensaje.

La disponibilidad del código fuente permite que la seguridad en Linux se evalué de forma abierta, lo que evita que se implementen modelos de seguridad pobres. Además, la mayoría de los proyectos de software libre tienen sistemas de revisión por terceras partes, que, como primera medida, evitan que se introduzcan en el sistema problemas de seguridad potenciales.

1.5.2 JUSTIFICACIÓN PRÁCTICA

Con la Red Privada Virtual, se va a permitir la conexión de los diferentes campamentos distantes de Caminosca S.A. para transmitir datos mediante un canal seguro de comunicación así como también la conexión de usuarios remotos hacia VPN con seguridad y confiabilidad.

1.6 ALCANCE DEL PROYECTO

La finalidad de la tesis, es realizar la conexión de una VPN bajo la plataforma de GNU/Linux. con un cliente que trabaja bajo la plataforma de Windows Xp.

Con una VPN, se podrá enlazar las redes distantes de la empresa Caminosca S.A. y también, autorizar la conexión de usuarios remotos, mediante métodos de autentificación y cifrado de datos de forma segura, esto se limitará a trabajar bajo GNU/LINUX para el servidor y Windows Xp para el cliente.

En la plataforma GNU/Linux se subirán los servicios necesarios para la implementación de la VPN.

Se realizarán pruebas hasta realizar la conexión y comprobar el correcto funcionamiento con los usuarios externos sin que existan problemas al momento de enviar y transmitir la información.

Se utilizará un servidor adquirido exclusivamente por la empresa para implementar el proyecto, en el cual se instalará y se configurará GNU/Linux para desarrollar la conexión.

El servidor VPN ubicado en la oficina matriz de Caminosca S.A., configurado de acuerdo a las necesidades de la empresa se conectará hacia un conmutador Core 3com 5500i Capa 3 Lan/Wan, esta información pasará por un firewall hasta el router Cisco 851, que se encuentra en el cuarto de telecomunicaciones del proveedor a través de fibra óptica, la información cifrada pasará hasta la red pública y llegará finalmente hasta la red de la sucursal de Caminosca.

Cabe recalcar que algunos de los dispositivos que se van a utilizar en el proyecto ya los posee la empresa por lo cual se aprovechará estos recursos para realizar lo planteado.

1.7 METODOLOGÍA

1.7.1 MÉTODO INDUCTIVO

Caminosca trabaja con varios proyectos a nivel nacional, con oficinas ubicadas en distintos lugares de la ciudad, por tal motivo entre los colaboradores es muy importante el intercambio de información día a día, y la comunicación entre ellos para saber los detalles y comentarios de cómo avanzan los proyectos, la comunicación es entre el correo y el ftp, en el cual la información puede perderse o puede ser filtrada, por tal motivo se vio la necesidad de investigar una mejor forma de hacer que toda esta información pueda llegar a los distintos colaboradores de las oficinas sucursales, de manera segura y como si estuvieran trabajando directamente desde la oficina matriz, y esto lo podríamos lograr con una conexión de red privada virtual.

1.7.2 MÉTODO DEDUCTIVO

Mediante la realización de este proyecto, se logrará la conexión de las oficinas sucursales con la oficina matriz mediante una red privada virtual, para que la información de los proyectos realizados pueda llegar a su destino y el intercambio de la misma sea fiable y segura, sin que se pueda perder o ser filtrada por otro tipo de personas ajenas a la empresa.

CAPÍTULO 2

CONCEPTOS BÁSICOS

En este capítulo, se revisará algunos conceptos básicos, funcionamiento y tipos de conexiones de una VPN, algunos protocolos, para así escoger las mejores alternativas para el funcionamiento de nuestra conexión VPN basado en Linux.

INTRODUCCIÓN

VPN (Virtual Private Network) es una extensión de una red local y privada que utiliza como medio de enlace una red pública como por ejemplo, Internet. También es posible utilizar otras infraestructuras WAN.

Este método permite enlazar dos o más redes simulando una única red privada permitiendo así la comunicación entre computadoras como si fuera punto a punto.

También un usuario remoto se puede conectar individualmente a una LAN utilizando una conexión VPN, y de esta manera utilizar aplicaciones, enviar datos, etc. de manera segura.

Las Redes Privadas Virtuales utilizan tecnología de túnel (tunneling) para la transmisión de datos mediante un proceso de encapsulación y en su defecto de encriptación, esto es importante a la hora de diferenciar Redes Privadas Virtuales y Redes Privadas, ya que esta última utiliza líneas telefónicas dedicadas para formar la red.

Esta tecnología es muy útil para establecer redes que se extienden sobre áreas geográficas extensas, por ejemplo diferentes ciudades y a veces hasta países y continentes. Por ejemplo empresas que tienen oficinas remotas en puntos distantes, la idea de implementar una VPN haría reducir notablemente los costos de comunicación.

2.1 REDES PRIVADAS VIRTUALES

2.1.1 CONCEPTO DE UNA VPN

Las redes de área local (LAN) son las redes internas de las organizaciones, es decir, las conexiones entre los equipos de una organización particular. Estas redes se conectan cada vez con más frecuencia a Internet mediante un equipo de interconexión. Muchas veces, las empresas necesitan comunicarse por Internet con filiales, clientes o incluso con el personal que puede estar alejado geográficamente.

Sin embargo, los datos transmitidos a través de Internet son mucho más vulnerables que cuando viajan por una red interna de la organización, ya que la ruta tomada no está definida por anticipado, lo que significa que los datos deben atravesar una infraestructura de red pública que pertenece a distintas entidades. Por esta razón, es posible que a lo largo de la línea, un usuario entrometido, escuche la red o incluso secuestre la señal. Por lo tanto, la información confidencial de una organización o empresa no debe ser enviada bajo tales condiciones.

La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas. Sin embargo, como la mayoría de las compañías no pueden conectar dos redes de área local remotas con una línea dedicada, a veces es necesario usar Internet como medio de transmisión.[1]

Una buena solución consiste en utilizar Internet como medio de transmisión con un protocolo de *túnel*, que significa que los datos se encapsulan antes de ser enviados de manera cifrada. El término Red privada virtual (abreviado VPN) se utiliza para hacer referencia a la red creada artificialmente de esta manera.

[1] http://ondinet.net/msm/index.php?option=com_k2&view=item&layout=item&id=19&Itemid=235

Se dice que esta red es virtual porque conecta dos redes "físicas" (redes de área local) a través de una conexión poco fiable (Internet) y privada porque sólo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden "ver" los datos.

Por lo tanto, el sistema VPN brinda una conexión segura a un bajo costo, ya que todo lo que se necesita es el hardware de ambos lados. Sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es pública y por lo tanto no está garantizada.

2.1.2 FUNCIONAMIENTO DE UNA VPN

Una red privada virtual se basa en un protocolo denominado protocolo de túnel, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.[2].

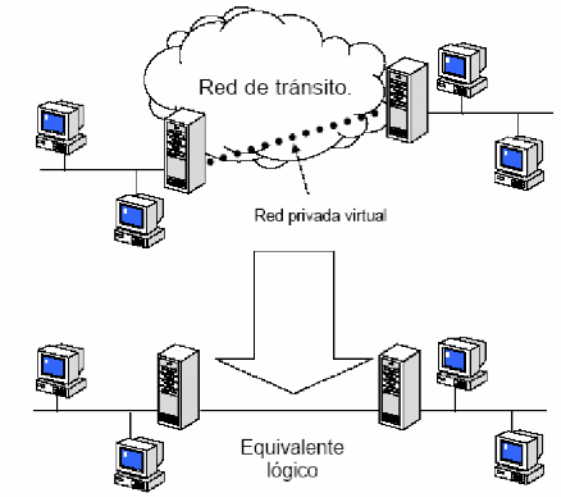

Figura 2.1 Funcionamiento de una VPN

Fuente: http://mantenimientodecomputadora.webs.com/tiposderedes.htm

La palabra "túnel" se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son

[2] http://mantenimientodecomputadora.webs.com/tiposderedes.htm

incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel.

En una *VPN* de dos equipos, el *cliente de VPN* es la parte que cifra y descifra los datos del lado del usuario y el *servidor VPN* (comúnmente llamado servidor de acceso remoto) es el elemento que descifra los datos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y este envía la respuesta cifrada.

Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario.

2.1.3 CARACTERÍSTICAS DE UNA VPN

Las redes virtuales privadas pueden encontrarse en los lugares de trabajo y en la casa y permiten a los empleados conectarse con seguridad a las redes de la empresa. Los trabajadores y aquellos que viajan con frecuencia, encuentran que las redes VPN son una forma más conveniente de permanecer conectados con la Intranet corporativa. Todo esto utilizando la infraestructura de Internet.

Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autentificación, integridad y confidencialidad de toda la comunicación.

2.1.3.1 Protección de los usuarios remotos

Una vez que OpenVPN ha establecido un túnel el firewall de la organización protegerá el equipo remoto aun cuando no es un equipo de la red local. Por otra parte, solo un puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.

2.1.3.2 Conexiones OpenVPN pueden ser realizadas a través de firewall

Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.

2.1.3.3 Soporte para proxy

Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor.

2.1.3.4 Solo un puerto en el firewall debe ser abierto para permitir conexiones

dado que desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo puerto TCP o UDP.

Las interfaces virtuales (tun0, tun1, etc.) permiten la implementación de reglas de firewall muy específicas.

2.1.3.5 Alta flexibilidad y posibilidades de extensión mediante scripting

OpenVPN ofrece numerosos puntos para ejecutar scripts individuales durante su arranque.

2.1.3.6 Soporte transparente para IPs dinámicas

Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.

2.1.3.7 Ningún problema con NAT

Tanto los clientes como el servidor pueden estar en la red usando solamente IPs privadas.

2.1.3.8 Instalación sencilla en cualquier plataforma

Tanto la instalación como su uso son increíblemente simples.

2.1.4 TIPOS DE VPN

Básicamente existen cuatro arquitecturas de conexión VPN: [3]

2.1.4.1 VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

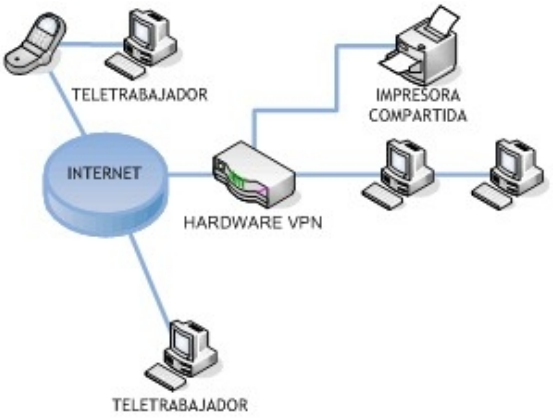

Figura 2. 2 Vpn Acceso remoto

Fuente: http://redprivadavirtualiut.wikispaces.com/Tipos+de+VPN

2.1.4.2 VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet,

[3] http://campusvirtual.unex.es/cala/cala/mod/resource/view.php?id=1875

acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a puntos tradicionales, sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

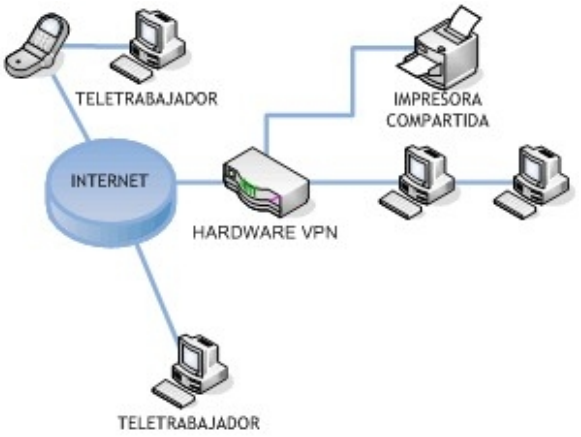

Figura 2. 3 Vpn Punto a punto

Fuente: http://redprivadavirtualiut.wikispaces.com/Tipos+de+VPN

2.1.4.3 Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (Unidad de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los

puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.[4]

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

2.1.4.4 VPN Interna VLAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

[4] http://redprivadavirtualiut.wikispaces.com/Tipos+de+VPN

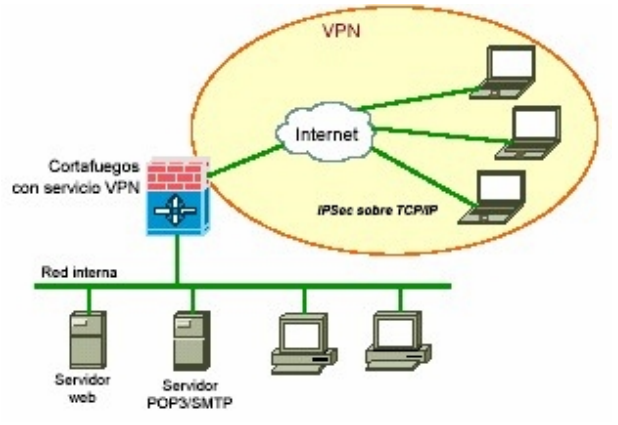

Figura 2. 4 Vpn Interna Lan

Fuente: http://redprivadavirtualiut.wikispaces.com/Tipos+de+VPN

2.1.5 SERVIDORES VPN

Tenemos varios servicios de los cuales nos permite crear estos túneles en GNU/Linux, los más conocidos son:

2.1.5.1 OpenVPN

Es una solución completa de conexión de redes VPN, contiene validación de usuario, enviado de informaron encriptado.

2.1.5.2 PPTP

Este el protocolo que realiza conexiones punto a punto, su principal habilidad la conexión múltiple de protocolos dentro del servicio.

2.1.5.3 Openswan

Es una implementación de IPSec, son varios protocolos cuya función es garantizar la comunicación sobre el protocolo de internet, permite la autenticación y cifrado.

2.2 BENEFICIOS DE UNA VPN

1. Ofrece conectividad a zonas geográficas
2. Mejora la seguridad
3. Reduce costes frente a otras soluciones WAN
4. Mejora la productividad
5. Simplifica las redes de datos
6. Abre un nuevo abanico de oportunidades
7. Favorece el soporte remoto
8. Es compatible con las conexiones de banda ancha

2.2.1 VENTAJAS DE LA VPN

- **Ahorro**.- Nos permite conectar redes físicamente separadas sin necesidad de usar una red dedicada, si no que a través de internet.
- **Transparencia**.- Interconectar distintas sedes es transparente para el usuario final, ya que la configuración se puede hacer sólo a nivel de pasarela.
- **Seguridad**.- Se pueden asegurar múltiples servicios a través de un único mecanismo.
- **Movilidad**.- Nos permite asegurar la conexión entre usuarios móviles y nuestra red fija.
- **Simplicidad**.- Este tipo de soluciones permite simplificar al administrador de la conexión de servidores y aplicaciones entre diferentes dominios.

2.3 REQUERIMIENTOS BÁSICOS DE UNA VPN

Por lo general, cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

AUTENTICACIÓN DE USUARIO

Se deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados solamente. También es conveniente llevar registros de quienes entran en la VPN y los horarios en que lo hacen.

ADMINISTRACIÓN DE DIRECCIÓN

Se deberá asignar una dirección al cliente en la red privada, y asegurarse de que las direcciones privadas se mantengan así.

ENCRIPTACIÓN DE DATOS

Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red para lo cual se usan técnicas de encriptación detalladas en este mismo trabajo. Entre las tareas en la encriptación de datos está la de generar y renovar las llaves de encriptación para el cliente y para el servidor.

ADMINISTRACIÓN DE CLAVES

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

SOPORTE DE PROTOCOLO MÚLTIPLE

La solución deberá manejar protocolos comunes utilizados en las redes públicas; éstos incluyen Protocolo de Internet. Una solución de VPN de Internet basada en un Protocolo de túnel de punto a punto o un Protocolo de túnel de nivel 2 (L2TP) cumple con todos estos requerimientos básicos, y aprovecha la amplia disponibilidad de Internet a nivel mundial.

2.4 PROBLEMAS DE SEGURIDAD

Es indispensable en una VPN generar una transmisión de datos que sea segura, en el caso del protocolo TCP/IP en particular se creó para que se tenga un alto grado de confiabilidad en la transmisión de los datos pero no a nivel seguridad,

los paquetes en Internet viajan sin encriptación alguna con lo cual no hay una privacidad (Sniffing) ni control de suplantación (Spoofing) de los datos que se transmiten por la misma.

Los problemas de seguridad son los siguientes:

ESCUCHAS CLANDESTINAS DE DATOS (SNIFFING).

Normalmente los dispositivos de una red solo toman los paquetes que le corresponden, el sniffing es una técnica por la cual una máquina de una red toma todos los paquetes que circulan por ella mas allá de que estén destinados o no para ella, accediendo de esa forma a toda la información que circule por la red.

SUPLANTACIÓN DE DATOS (SPOOFING).

En esta técnica una terminal emula a otra. El usuario fuerza a la computadora a tomar los certificados de otra. De esta forma está capacitada para enviar mensajes a un dispositivo teniendo la posibilidad de acceder a una red a la cual no pertenezca y enviando mensajes que para las demás estaciones de trabajo parecen legítimos.[5]

CAPTURA DE DIRECCIONES.

Los paquetes que se transmiten contienen información en los encabezados y en el cuerpo que pueden ser direcciones de servidores, DNS, proxys, estaciones de trabajo y de todos los dispositivos de red.

2.5 DISEÑO DE UNA VPN

Para realizar el diseño de una Red Privada Virtual se utilizará algunos elementos que se detallan a continuación:

[5] http://www.textoscientificos.com/redes/redes-virtuales/vpn

- **Servidor VPN.-** es el elemento que descifra los datos del lado de la organización. Un computador que recibe conexiones VPN de clientes VPN mediante acceso remoto o conexiones de enrutador a enrutador**.**
- **Cliente VPN.-** es la parte que cifra y descifra los datos del lado del usuario. Un computador que inicia un enlace o conexión a un servidor VPN.
- **Conexión VPN.-** Es la parte del enlace en la cual los datos encriptados para obtener una conexión más segura, los datos deben ser encriptados a los largo de toda la conexión VPN.

- **Red Pública.-** Permite la conexión VPN a través de la cual los datos viajan encapsulados.
- **Switch.-** es un dispositivo de conmutación que permite el control de distintos equipos con tan sólo un monitor, un teclado y un ratón. **Router.-** Dispositivo hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.
- **Concentradores.-** es un elemento de hardware que permite concentrar el tráfico de red que proviene de múltiples hosts y regenerar la señal. El concentrador es una entidad que cuenta con determinada cantidad de puertos (posee tantos puertos como equipos a conectar entre sí. Su único objetivo es recuperar los datos binarios que ingresan a un puerto y enviarlos a los demás puertos. Al igual que un repetidor, el concentrador funciona en el nivel 1 del modelo OSI. Es por ello que a veces se lo denomina repetidor multipuertos.
- **Firewall.-** Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

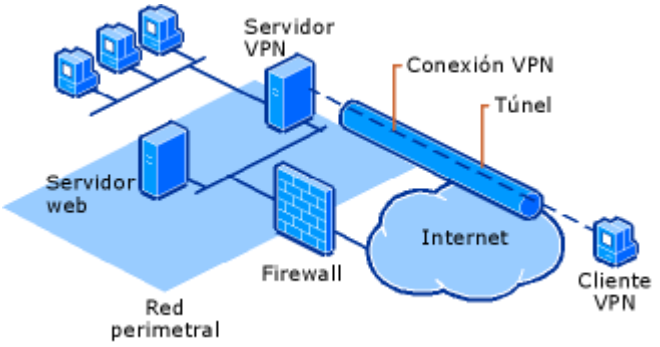

Figura 2. 5 Conexión Vpn con firewal

Fuente: http://technet.microsoft.com/es-es/library/cc753364%28v=ws.10%29l

2.5.1.1 Configuración de la VPN

VPN (Virtual Private Network) significa literalmente Red Privada Virtual. Básicamente consiste en realizar una conexión a una red externa creando un túnel a través de internet, permitiendo la creación de una red privada dentro de una red pública.[6]

Cuando el equipo es servidor y miembro de un dominio, para configurar conexiones entrantes tiene que utilizar la herramienta Enrutamiento y acceso remoto. El uso de esta herramienta puede ayudar a configurar redes privadas virtuales y conjuntos de módems en un servidor de acceso remoto.

El Asistente para la instalación del servidor de Enrutamiento y acceso remoto se utiliza para configurar tipos de servidores de acceso remoto comunes, como servidores de redes privadas virtuales.

2.6 TÚNELES

2.6.1 TÚNEL

De túnel se utiliza para describir un método que utiliza una infraestructura de red interna para la transferencia de una carga útil. Túnel también se conoce como la

[6] http://www.configurarequipos.com/doc499.html

encapsulación y la transmisión de datos VPN, o paquetes. El modo de túnel IPSec permite cargas de propiedad intelectual a cifrar y encapsulado en un encabezado IP para que se pueda enviar por la red interna IP de empresa o de Internet.

Aunque, por definición, un túnel no está cifrado, por lo general la razón de usar uno, es que se desea añadirle alguna clase de cifrado. Dado que los datos que se transfieren entre las oficinas son probablemente sensibles, no se deseará que alguien sea capaz de ver los datos mientras viajan a través de Internet, muchas personas lo utilizan el túnel para cifrar una conexión TCP / IP desde una aplicación a un servidor.

Algunas aplicaciones, sobre todo las basadas en un protocolo cliente / servidor, necesita conectarse a un servidor de base de datos para acceder a sus datos. El uso de un túnel es una excelente manera no sólo de hacer la conexión más fácil para el usuario final, sino también de asegurar las comunicaciones.

2.7 PROTOCOLOS

2.7.1 PROTOCOLO

Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red. Un protocolo es una convención o estándar que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. En su forma más simple, un protocolo puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos. A su más bajo nivel, un protocolo define el comportamiento de una conexión de hardware.[6]

2.7.1.1 PPP: Protocolo punto a punto

El protocolo **PPP** proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto entre dos "pares". Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

Funcionamiento general

Para dar un panorama inicial del funcionamiento de este protocolo en el caso comentado, en que un usuario de una PC quiera conectarse temporalmente a Internet, describiremos brevemente los pasos a seguir:

En primera instancia, la PC llama al router del **ISP** (Internet Service Provider, proveedor del servicio de Internet), a través de un módem conectado a la línea telefónica.

Una vez que el módem del router ha contestado el teléfono y se ha establecido una conexión física, la PC manda al router una serie de paquetes LCP en el campo de datos de uno o más marcos PPP. Estos paquetes y sus respuestas seleccionan los parámetros PPP por usar.

Una vez que se han acordado estos parámetros se envían una serie de paquetes NCP para configurar la capa de red.

Típicamente, la PC quiere ejecutar una pila de protocolos TCP/IP, por lo que necesita una dirección IP. No hay suficientes direcciones IP para todos, por lo que normalmente cada ISP tiene un bloque de ellas y asigna dinámicamente una a cada PC que se acaba de conectar para que la use durante su sesión. Se utiliza el NCP para asignar la dirección de IP.

En este momento la PC ya es un host de Internet y puede enviar y recibir paquetes IP. Cuando el usuario ha terminado se usa NCP para destruir la conexión de la capa de red y liberar la dirección IP.

Luego se usa LCP para cancelar la conexión de la capa de enlace de datos.

Finalmente la computadora indica al módem que cuelgue el teléfono, liberando la conexión de la capa física.

PPP puede utilizarse no solo a través de líneas telefónicas de discado, sino que también pueden emplearse a través de SONET o de líneas HDLC orientadas a bits.[7]

2.7.1.2 PPTP (Point to Point Tunneling Protocol)

Este es uno de los protocolos más populares y fue originalmente diseñado para permitir el transporte (de modo encapsulado) de protocolos diferentes al TCP/IP a través de Internet.

Básicamente, PPTP lo que hace es encapsular los paquetes del protocolo punto a punto PPP (Point to Point Protocol) que a su vez ya vienen encriptados en un paso previo para poder enviarlos a través de la red.

El proceso de encriptación es gestionado por PPP y luego es recibido por PPTP, este ultimo utiliza una conexión TCP llamada conexión de control para crear el túnel y una versión modificada de la Encapsulación de Enrutamiento Genérico (GRE, Generic Routing encapsulation) para enviar los datos en formato de datagramas IP, que serian paquetes PPP encapsulados, desde el cliente hasta el servidor y viceversa.

El proceso de autenticación de PPTP utiliza los mismos métodos que usa PPP al momento de establecer una conexión, como por ejemplo PAP (Password Authenticaction Protocol) y CHAP (Challenge-Handshake Authentication Protocol).

El método de encriptación que usa PPTP es el Microsoft Point to Point Encryption, MPPE, y solo es posible su utilización cuando se emplea CHAP (o MS-CHAP en los NT) como medio de autenticación.

---

[7] http://www.lugro.org.ar/biblioteca/articulos/vpn_intro/vpn_intro.html

Es posible establecer conexiones mediante túneles sin encriptación, es decir, realizar solamente la Encapsulación, pero esto no está considerado que sea una VPN ya que los datos viajan de forma insegura a través de la red.

2.7.1.3 Diagramas

Hay varias posibilidades de conexiones VPN, esto será definido según los requerimientos de la organización, por eso es aconsejable relevar información a fin de obtener datos como por ejemplo si lo que se desea enlazar son dos o más redes, o si solo se conectaran usuarios remotos.

Las posibilidades son:

- **DE CLIENTE A SERVIDOR (Client to Server):**

Un usuario remoto que solo necesita servicios o aplicaciones que corren en el mismo servidor VPN.

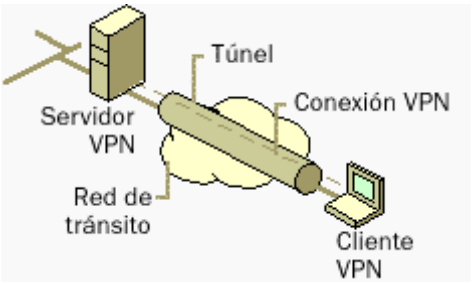

Figura 2. 6 Conexión de cliente a servidor

Fuente: www.lugro.org.ar/biblioteca/articulos/vpn_intro/vpn_intro.html

- **DE CLIENTE A RED INTERNA (Client to LAN):**

Un usuario remoto que utilizara servicios o aplicaciones que se encuentran en uno o más equipos dentro de la red interna.

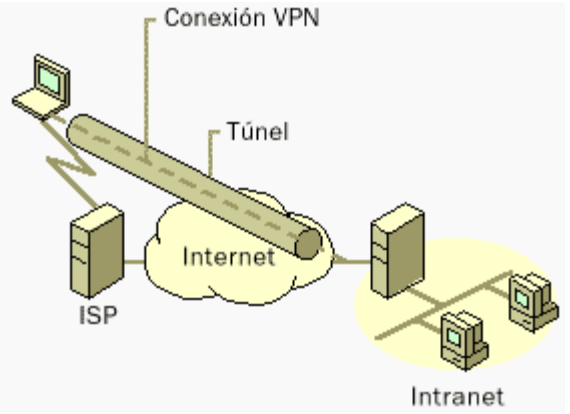

Figura 2.7 Conexión de cliente a red interna

Fuente: www.lugro.org.ar/biblioteca/articulos/vpn_intro/vpn_intro.html

- **DE RED INTERNA A RED INTERNA (LAN to LAN):**

Esta forma supone la posibilidad de unir dos intranets a través de dos enrutadores, el servidor VPN en una de las intranets y el cliente VPN en la otra.

Aquí entran en juego el mantenimiento de tablas de ruteo y enmascaramiento.

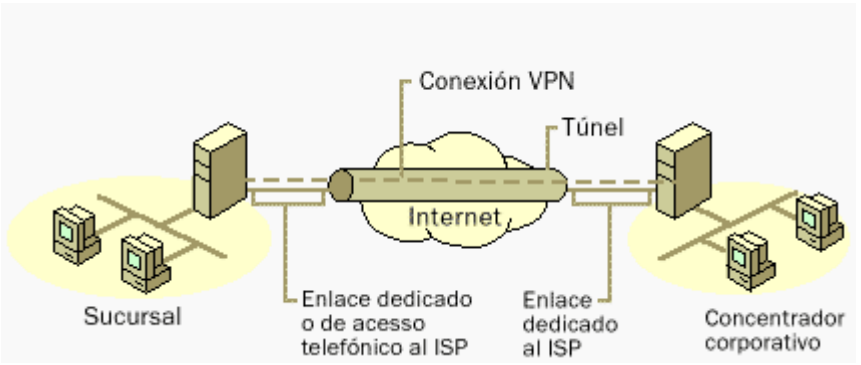

Figura 2.8 Conexión de red interna a red interna

Fuente: www.lugro.org.ar/biblioteca/articulos/vpn_intro/vpn_intro.html

2.7.1.4 IPSEC (Internet Protocol Security)

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión. Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos. Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP.

2.7.1.5 L2TP (Layer 2 Tunneling Protocol)

Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local. [8]

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel. [8]

Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

---

[8] http://www.slideshare.net/paulguachamin/vpn-7863465

2.7.1.6 SOCKS (Networks Security Protocol)

Es un protocolo de Internet que permite a las aplicaciones Cliente-servidor usar de manera transparente los servicios de un firewall de red. SOCKS es una abreviación de "SOCKETS".

Los clientes que hay detrás de un firewall, los cuales necesitan acceder a los servidores del exterior, pueden conectarse en su lugar a un servidor proxy SOCKS. Tal servidor proxy controla que cliente puede acceder al servidor externo y pasa la petición al servidor. SOCKS puede ser usado también de la forma contraria, permitiendo a los clientes de fuera del firewall ("clientes exteriores") conectarse a los servidores de dentro del firewall (servidores internos). [9]

2.7.1.7 SSL (Secure Sockets Layer)

El protocolo SSL (Secure Sockets Layer) permite establecer conexiones seguras a través de Internet, de forma sencilla y transparente. La idea consiste en interponer una fase de codificación de los mensajes antes de enviarlos por la red. Una vez que se ha establecido la comunicación, cuando una aplicación quiere enviar información a otra computadora, la capa SSL la recoge y la codifica, para luego enviarla a su destino a través de la red. Análogamente, el módulo SSL del otro ordenador se encarga de decodificar los mensajes y se los pasa como texto plano a la aplicación destino.

Cada sesión SSL lleva asociado un identificador único que evita la posibilidad de que un atacante escuche la red y repita exactamente lo mismo que ha oído, aún sin saber lo que significa, para engañar a uno de los interlocutores.

Las ventajas de este protocolo son evidentes, ya que liberan a las aplicaciones de llevar a cabo las operaciones criptográficas antes de enviar la información, y su transparencia permite usarlo de manera inmediata sin modificar apenas los programas ya existentes.

---

[9] http://www.linuxparatodos.net/portal/article.php?story=sockets

Desgraciadamente, las versiones de exportación tanto de Netscape como de Internet Explorer trabajan con claves de sesión de 40 bits, que pueden ser descifradas en cuestión de pocas horas por cualquier PC más o menos potente, por lo que en ningún caso pueden ser merecedoras de nuestra confianza.

2.7.1.8 TLS (Transport Layer Secutiry)

El protocolo TLS (Transport Layer Security) es una evolución del protocolo SSL (Secure Sockets Layer). [10]

Los objetivos del protocolo son varios:

1. **Seguridad criptográfica.** El protocolo se debe emplear para establecer una conexión segura entre dos partes.
2. I**nteroperabilidad.** Aplicaciones distintas deben poder intercambiar parámetros criptográficos sin necesidad de que ninguna de las dos conozca el código de la otra.
3. **Extensibilidad.** El protocolo permite la incorporación de nuevos algoritmos criptográficos.
4. **Eficiencia.** Los algoritmos criptográficos son costosos computacionalmente, por lo que el protocolo incluye un esquema de cache de sesiones para reducir el número de sesiones que deben inicializarse desde cero (usando criptografía de clave pública).[10]

El protocolo está dividido en dos niveles:

- Protocolo de registro TLS (TLS Record Protocol).
- Protocolo de mutuo acuerdo TLS (TLS Handshake Protocol).

El de más bajo nivel es el Protocolo de Registro, que se implementa sobre un protocolo de transporte fiable como el TCP. El protocolo proporciona seguridad en la conexión con dos propiedades fundamentales:

---

[10] http://www.uv.es/sto/cursos/seguridad.java/html/sjava-25.html

1. **La conexión es privada**. Para encriptar los datos se usan algoritmos de cifrado simétrico. Las claves se generan para cada conexión y se basan en un secreto negociado por otro protocolo (como el de mutuo acuerdo). El protocolo también se puede usar sin encriptación.

2. **La conexión es fiable.** El transporte de mensajes incluye una verificación de integridad.

El protocolo de registro se emplea para encapsular varios protocolos de más alto nivel, uno de ellos, el protocolo de mutuo acuerdo, permite al servidor y al cliente autentificarse mutuamente y negociar un algoritmo de encriptación y sus claves antes de que el protocolo de aplicación transmita o reciba datos.[11]

El protocolo de mutuo acuerdo proporciona seguridad en la conexión con tres propiedades básicas:

1. La identidad del interlocutor puede ser autentificada usando criptografía de clave pública. Esta autentificación puede ser opcional, pero generalmente es necesaria al menos para uno de los interlocutores.
2. La negociación de un secreto compartido es segura.
3. La negociación es fiable, nadie puede modificar la negociación sin ser detectado por los interlocutores.

2.7.1.9 SSH (Secure Shell)

SSH (Secure Shell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos.[12]

---

[11] http://www.ecured.cu/index.php/TLS

[12] http://www.flu-project.com/configuracion-servidor-ssh-en-gnulinux.html

Además de la conexión a otros dispositivos, SSH permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

2.7.1.10 Asociación de Seguridad (SA)

Es el establecimiento de los atributos de seguridad compartidos entre dos entidades de la red de apoyo a la comunicación segura. Una SA puede incluir características tales como: el algoritmo de cifrado, y el modo de clave de cifrado del tráfico, y los parámetros para los datos de la red para ser pasado por alto la conexión. El marco para el establecimiento de asociaciones de seguridad es proporcionado por la Asociación de Internet Security and Key Management Protocol (ISAKMP). Protocolos como el Internet Key Exchange y negociación de claves Kerberos de Internet proporcionan material de claves autenticado.

Una SA es (un solo sentido de canal) y la conexión lógica que respalda y proporciona una conexión segura de datos entre los dispositivos de red. El requisito fundamental de una SA llega cuando las dos entidades se comunican a través de más de un canal. Tomemos un ejemplo del móvil de abonado y una estación base . El abonado puede en sí suscribir más de un servicio. Por tanto, cada servicio puede tener diferentes primitivas de servicio como un algoritmo de cifrado de datos, clave pública o el vector de inicialización. Ahora, para facilitar las cosas, toda esta información de seguridad se agrupan de forma lógica. Este grupo de lógica en sí es una asociación de seguridad. Cada SA tiene su propio ID llama SAID. Así que ahora la estación base y el abonado móvil a compartir lo dicho y lo que va a obtener todos los parámetros de seguridad, haciendo las cosas mucho más fácil.

2.7.1.11 Internet Key Exchange (IKE)

El protocolo para Intercambio de Claves en Internet es el encargado en la infraestructura IPSec de proporcionar un entorno previo seguro para la compartición de una clave secreta y autenticación de los extremos. IKE utiliza el puerto 500 de UDP para establecer el intercambio de mensajes pertinente. Por lo

general se implementa como una aplicación en espacio de usuario, al no formar parte del núcleo de muchos sistemas operativos.

Se compone de dos fases diferenciadas. La primera de ellas efectúa el intercambio de mensajes preliminares necesarios, estableciendo una asociación de seguridad ISAKMP (ISAKMP SA). Este intercambio inicial puede estar basado en claves pre compartidas o PSK, claves RSA para criptografía asimétrica, o una infraestructura PKI de certificados digitales.

2.7.1.12 Internet Key Exchange (IKE o IKEv2)

Es el protocolo utilizado para establecer una asociación de seguridad (SA) en el IPsec conjunto de protocolos. IKE se basa en el protocolo Oakley y ISAKMP . IKE utiliza X.509 certificados para la autenticación, que son pre-compartidos o distribuidos usando DNS (de preferencia con DNSSEC), y un intercambio de claves Diffie-Hellman para establecer una sesión secreta compartida desde el que las claves criptográficas se derivan.

Además, una política de seguridad para todos los pares que se conectará de forma manual debe ser mantenida.

2.8 TIPOS DE CONEXIÓN

2.8.1 CONEXIÓN DE ACCESO REMOTO

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

2.8.2 CONEXIÓN VPN ROUTER A ROUTER

Una conexión VPN es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica

ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.[13]

2.8.3 CONEXIÓN VPN FIREWALL A FIREWALL

Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.[12]

2.9 ARQUITECTURA DE LAS VPN

Dentro de las posibles arquitecturas que están en las VPN se pueden mencionar las siguientes:

- **PROPORCIONADA POR UN SERVIDOR DE INTERNET**

El proveedor de Internet puede instalar en su oficina un dispositivo que se encargara de la creación del túnel para la organización.

- **BASADAS EN FIREWALLS**

De la misma forma en que las VPN trabajan en los niveles más bajos del modelo OSI, el firewall actuará de la misma forma.

- **BASADAS EN CAJA NEGRA**

Básicamente es un dispositivo con software de encriptación. No provee seguridad en la organización pero si en los datos. Para suplir esta falencia se pueden utilizar un firewall en serie o paralelo al dispositivo de VPN.

---

[13] http://profecarolinaquinodoz.com/principal/?tag=concepto-de-red-vpn

- **BASADAS EN ROUTERS**

Puede ser en este caso que el software de encriptación se añada al router ya existente o bien que se utilice una salida exclusiva de otro proveedor.

- **BASADAS EN ACCESO REMOTO**

El cliente tiene software por el cual se conecta al servidor de VPN de la corporación a través de un túnel encriptado.

- **BASADAS EN SOFTWARE**

Por lo general, se utiliza de un cliente a un servidor de VPN que está instalado en alguna estación de trabajo. Es necesario tener procesos de administración de claves y un emisor de certificados.

- **SEGURIDADES DE UNA VPN**

Toda la seguridad representa un balance que actué entre la protección contra amenazas de seguridad potenciales y el no saturar la red o el desempeño organizacional, de las empresas, es de suma importancia para cualquier compañía que realice negocios a través de internet la seguridad de las VPN'S.

Todos los procedimientos normales de seguridad se aplican a las VPN's como lo harían a cualquier dispositivo de red, además de estos procedimientos normales de seguridad, se requieren procesos de seguridad debido a la singularidad de la tecnología VPN.

Los factores a tomarse en cuenta el momento de proveer seguridades a una VPN son los siguientes: cifrado, dispositivos VPN, autentificación, el proceso sin rechazos, el cifrado punto a punto, la administración centralizada de la seguridad y los procedimientos de respaldo/restauración.

Los criterios y medidas que componen la seguridad de una VPN son las siguientes:

Los datos de la VPN viajan a través de una red pública, por lo que cualquier persona no autorizada tendrá la capacidad para interceptarlos; por lo que el resguardo de estos se encuentra principalmente en la encriptación, la misma que provee normas de autentificación, cifrado e integridad para prevenir este hecho.

Sólo los usuarios autorizados pueden acceder a los recursos o aplicaciones existentes en los servidores corporativos, los usuarios deben tener distintos niveles de acceso. [14]

El servidor VPN debe proporcionar una administración fácil, que permita una configuración directa, mantenimiento y una actualización de las VPN'S de manera confiable.

2.10 SISTEMA OPERATIVO GNU/LINUX

2.10.1 DEFINICIÓN LINUX

Linux es un sistema operativo de software libre (no es propiedad de ninguna persona o empresa), por ende no es necesario comprar una licencia para instalarlo y utilizarlo en un equipo informático. Es un sistema multitarea, multiusuario, compatible con UNIX, y proporciona una interfaz de comandos y una interfaz gráfica, que lo convierte en un sistema muy atractivo y con estupendas perspectivas de futuro.

Al ser software libre, el código fuente es accesible para que cualquier usuario pueda estudiarlo y modificarlo. La licencia de Linux no restringe el derecho de venta, por lo que diversas empresas de software comercial distribuyen versiones de Linux. Además de esto, este sistema cuenta con muchas distribuciones y gestores de ventanas para el entorno gráfico.

El sistema operativo Linux fue desarrollado por Linus Torvalds, y se basa en el sistema Minix que a su vez está basado en el sistema Unix, Torvalds fue

---

[14] http://www.pandasecurity.com/NR/rdonlyres/6647F8ED-F5EA-4E73-AA5C-9B038B71F916/3176/VPN_spa_010205_2146481243.pdf

añadiéndole herramientas y utilidades, haciéndolo operativo. A partir de la primera versión de Linux el sistema ha sido modificado por miles de programadores de todo el mundo, bajo la coordinación de su creador.

El nombre de Linux proviene del nombre de su autor Linus y del sistema operativo UNIX. No obstante, su verdadero nombre es GNU/Linux, ya que el sistema se distribuye bajo licencia GNU GPL (General Public License).

La estructura del Linux está basada en un micronúcleo híbrido que ejecuta los servicios más básicos del sistema operativo. El Kernel es el núcleo del sistema; la parte que interactúa directamente con el hardware, administrando todos los recursos de éste, como la memoria, el microprocesador, los periféricos, etc.

Además, tiene un programa que aísla al usuario del núcleo, conocido como Shell o intérprete de comandos, su función es interpretar las órdenes o aplicaciones que el usuario mande al sistema, desde una terminal en modo texto o desde un entorno gráfico, y traducirlas a instrucciones que el sistema operativo entienda.

Dependiendo de su versión este sistema operativo se utiliza en supercomputadoras y servidores como computadoras personales. Las diferentes variantes del Linux se denominan distribuciones, entre los más conocidos se encuentran Red Hat-Fedora, Suse, Debian, Ubuntu, y Mandriva.

Cada distribución de Linux distribuye el núcleo mediante las actualizaciones del sistema operativo. Cada versión del núcleo se puede distinguir por 3 o 4 números separados por puntos. El significado de cada número es el siguiente:

1. Versión del núcleo; varía si hay una gran modificación en el código del núcleo.
2. Principal revisión del núcleo.

3. Revisión menor, como la inclusión de nuevos drivers o algunas características nuevas.

4. Correcciones de errores o fallos de seguridad dentro de una misma revisión.

Linux ha avanzado mucho en los últimos años, añadiendo mejoras en las interfaces gráficos de usuario, y en el reconocimiento y utilización de los recursos hardware. Poco a poco va ganándole terreno a Windows y a Unix, se ha convertido en el favorito de los usuarios de computadoras y de negocios expertos (empresas como IBM o Hewlett-Packard) que lo consideran una alternativa robusta y de bajo costo en comparación con los otros sistemas operativos; y prestan el soporte técnico correspondiente, normalmente como parte de los sistemas servidores.[15]

Para los creadores de Unix, un sistema operativo debería ser un conjunto de herramientas y conceptos básicos que le permitan al usuario construir rápida y fácilmente sus propias herramientas para automatizar procesos. Unix es como un juego de herramientas que puede aprovecharse al máximo con algo de estudio.

Otra gran idea que se ha desarrollo junto con Unix ha sido Internet, porque en este sistema se realizaron las primeras implementaciones de los protocolos de comunicación en los que se basa Internet, y aún hoy son sistemas Unix los que mantienen Internet en funcionamiento.

[15] http://conceptodefinicion.de/linux/

CAPÍTULO 3

ANÁLISIS DE REQUERIMIENTOS

En este capítulo, se analizará todos los requerimientos que la empresa tiene en la actualidad tanto en hardware como en software las plataformas de trabajo que utilizan para trabajar en sus servidores, se revisará los requerimientos, protocolo y software que se utilizan para configurar la Red Privada Virtual.

3.1 INFRAESTRUCTURA ACTUAL DE LA EMPRESA

La estructura física de la red se ubica en las oficinas de Caminosca, la misma que fue configurada para permitir la adaptación de nuevas tecnologías y el crecimiento de la misma.

En el Centro de cómputo donde están ubicados los equipos está constituido por los siguientes elementos:

3.1.1 HARDWARE

HARDWARE	CARACTERÍSTICAS
Servidor Principal	TYANthunder n6650w (s2915) 2 procesadores AMD Opteron 2220 EC RAM ddr2 eec 667 disco 800 GB
Servidor de Aplicaciones	Intel STL2, 2 pentium III 1 GHz Ram de 2000Mb Disco de 618 GB

Servidor de Base de Datos	Intel Xeon 2 Intel xeon 2.4 Ghz Ram de 3000 Mb Disco 108 Gb
Servidor Web FTP	Intel D845GRG RAM 1024 Mb Disco 36 GB
Switch Principal	SuperStack 4 Switch 5500-S1 28-Port 3 Com
9 Switch	D Link Switch DGS-1224T 3 Com Switch baseline 3 Com Switch 4228G 3 Com Switch SS 3870 24/P D link Switch DGS-1248T 48/P 4 Switch 3 Com Switch (4200 G)
Router	Cisco router 851

Tabla 3.1 Características del Hardware Cuarto de cómputo

Fuente: Cuarto de servidores de las oficinas de Caminosca

3.1.2 SOFTWARE

En el siguiente cuadro, se detalla las características de los servidores que se encuentran en el cuarto de cómputo.

SERVIDORES	SISTEMA OPERATIVO	SOFTWARE DE APLICACIONES
Servidor Principal	Windows Server 2008 Standar	
Servidor Web	Windows XP	Microsoft Office XP Std. Adobe Distiller 6.0
Servidor de Base de Datos	Windows Server 2000	SQL server 2000
Servidor de Aplicaciones	Linux Debian	Postgre SQL 8.1

Tabla 3.2 Características del Software Cuarto de cómputo

Fuente: Cuarto de servidores de las oficinas de Caminosca

3.1.3 DETALLE DE LOS EQUIPOS QUE CONFORMAN LA RED MATRIZ

En la siguiente figura, se describe la red que usa actualmente la empresa.

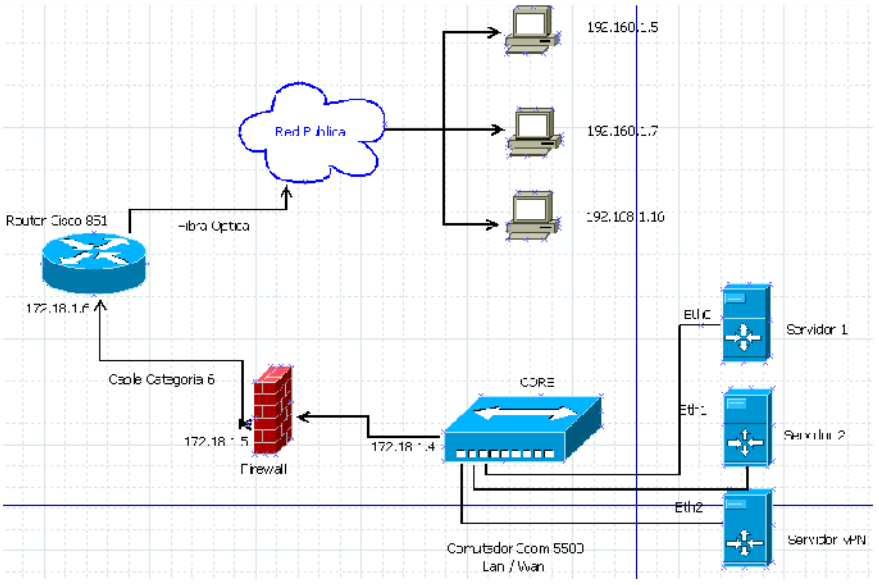

Figura 3.1 Diagrama de los equipos de la red matriz

Fuente: Información proporcionada por el administrador de la red

3.1.4 DETALLE DE LOS EQUIPOS QUE CONFORMAN LA RED SUCURSAL

En la siguiente figura, se detalla la red que se usa para las oficinas sucursales de la empresa. [16]

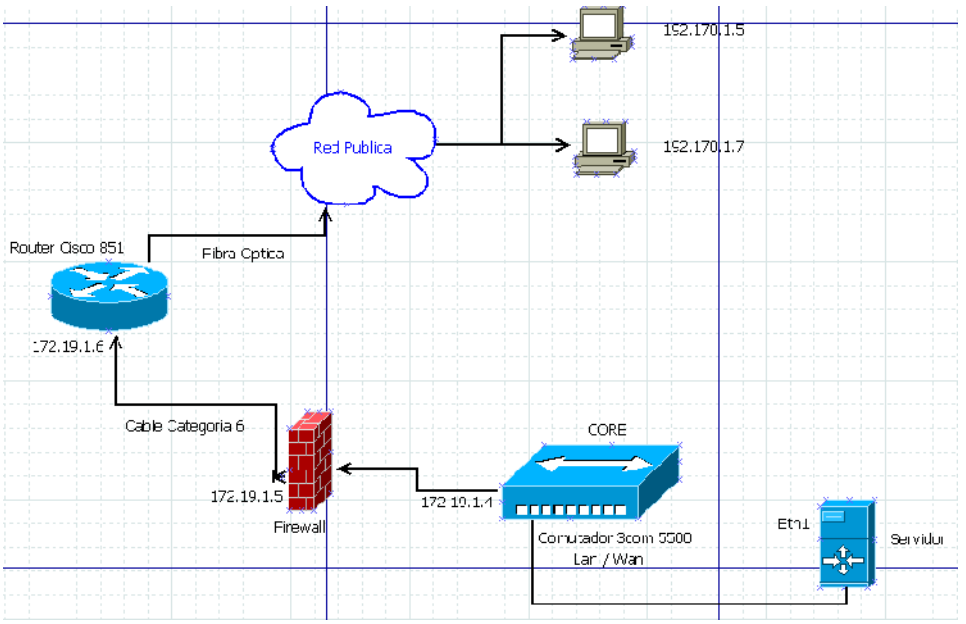

Figura 3.2 Diagrama de los equipos de la red sucursal

Fuente: Información proporcionada por el administrador de la red

3.2 TRANSFERENCIA DE INFORMACIÓN

En la actualidad la oficina matriz y las oficinas sucursales hacen transferencias de información, mediante mails, USB, Cd, y medios de almacenamiento externos, con el fin de consolidar dicha información, ya que las oficinas sucursales no acceden al servidor principal. En esta modalidad no se tienen las seguridades necesarias para el manejo de la información.

[16] Información proporcionada por el administrador de la Red

Por todo lo expuesto, se hace necesario desarrollar una Red Privada Virtual que permita comunicar a la oficina matriz con las oficinas sucursales, para evitar que la información este propensa a perderse o ser interferida.

3.3 ALTERNATIVAS DE SOLUCIÓN

Algunas empresas emplean soluciones de hardware VPN para aumentar la seguridad del manejo de toda su información, otras utilizan implementaciones basadas en software o protocolos.

3.3.1 HARDWARE

Hardware es el substrato físico en el cual existe el software. El hardware abarca todas las piezas físicas de un ordenador (disco duro, placa base, memoria, tarjeta aceleradora o de vídeo, lectora de CD, microprocesadores, entre otras). Sobre el hardware es que corre el software que se refiere a todos los programas y datos almacenados en el ordenador.

Se refiere a todos los aparatos, tarjetas (circuitos impresos electrónicos), y demás objetos físicos de los que está compuesto un PC.

3.3.1.1 SWITCH 3COM

La familia 3Com Switch 5500 incluye switches de última generación Fast Ethernet para Capa 2/3/4, los cuales son ideales para las más demandantes aplicaciones del Centro de Computo. Ofrecen conectividad flexible y escalable para una mezcla heterogénea de datos, voz y video, y otros servicios críticos para el negocio, y son particularmente idóneos para la construcción de arquitecturas de alta disponibilidad y "resilient". Estos modelos Switch 5500 vienen con 24 ó 48 puertos 10/100 más cuatro puertos activos Gigabit basados en SFP (Small Form-factor Plug-in).

- **CARACTERÍSTICAS**

    - El rendimiento a velocidad de cable en todos los puertos de una pila ofrece ancho de banda óptimo para datos críticos para la empresa y comunicaciones de alta velocidad.
    - Ancho de banda de apilamiento de 48 Gbps (96 Gbps full-dúplex) (modelos 10/100/1000).
    - Diseño escalable y apilable en ambos formatos Fast Ethernet y Gigabit Ethernet.
    - Están disponibles módulos 10-Gigabit Ethernet, para interconectar switches de núcleo y de distribución.

3.3.1.2 Swicth de VPN H3COM Tiping Point

TippingPoint™ de la división TippingPoint de 3Com es la primer plataforma de seguridad integrada, basada en la tecnología Intrusion Prevention System (IPS), que combina un firewall de inspección del estado de los paquetes, VPN IPSec, administración de ancho de banda, filtración de contenido de la Web y routing dinámico. Esta nueva plataforma satisface la creciente demanda de los clientes empresariales de contar con una solución de seguridad más completa que brinde una protección con la iniciativa, automatización y dinamismo que no ofrecen algunos firewalls.

CARACTERÍSTICAS

- **Prevención completa de intrusiones**

  Provee inspección profunda de paquetes Layer 2-7, contra ataques internos y externos, incluyendo vulnerabilidades por gusanos, virus, caballos de Troya, spyware, amenazas de par a par, phishing y día cero.

- **Servicios de seguridad integrados**

  Extiende la funcionalidad de un sistema de prevención de intrusos basado en redes con IPSec VPN, firewall de inspección de estado de paquetes,

administración de ancho de banda, routing dinámico y filtración de contenido, sin degradar el desempeño de la red.

- **Filtración de contenido**

  Impone el cumplimiento de políticas de los usos aceptables de la Web, para mejorar la productividad, disminuir el desperdicio de ancho de banda, reducir el potencial de responsabilidad y hacer que las corporaciones cumplan con los requerimientos legales.

- **Capacidades VoIP**

  Ofrece una prevención total de vulnerabilidades de la VoIP por medio de filtros de Digital Vaccine® de TippingPoint, además de facilitar el uso de sistemas VoIP basados en las oficinas centrales por las oficinas sucursales remotas. El establecimiento de prioridades de tráfico permite alta calidad de servicio (QoS) para las llamadas de VoIP en el túnel de la VPN.

3.2.2 SOFTWARE

Es el equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

El software es el método más seguro de establecer una red privada virtual entre sitios, proveen un método mejorado pasa los usuarios remotos.

Se analizará el software cliente y servidor para tener una mejor referencia.

3.2.2.1 Linux Debian (SERVIDOR)

Debian es una comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre. El sistema se encuentra precompilado, empaquetado y en un formato que puede usarse para múltiples arquitecturas de computador y para varios núcleos.

CARACTERÍSTICAS

Debian se caracteriza por:

- La disponibilidad en varias plataformas hardware. La versión 3.1a es compatible con 11 plataformas.
- Una amplia colección de software disponible. La versión 3.1a viene con unos 15490 paquetes de software|paquetes.
- Un grupo de herramientas para facilitar el proceso de instalación y actualización del software.
- Su compromiso con los principios y valores involucrados en el movimiento del Software Libre.
- No tiene marcado ningún entorno gráfico en especial, ya sea GNOME, KDE u otro.
- Un grupo de herramientas para facilitar el proceso de instalación y actualización del software (APT, Aptitude, Dpkg, Synaptic, Dselect, etc.) Todas ellas obtienen información de donde descargar software desde /etc./apt/sources.list, que contiene los repositorios.
- Su compromiso con los principios y valores involucrados en el movimiento del Software Libre.[17]

3.2.2.2 Windows XP Professional (CLIENTE)

Es una versión de Microsoft Windows, línea de sistemas operativos desarrollado por Microsoft. Lanzado al mercado el 25 de octubre de 2001.

Tiene una interfaz gráfica de usuario (GUI) perceptiblemente reajustada (denominada Luna), la cual incluye características rediseñadas, algunas de las cuales se asemejan ligeramente a otras GUI de otros sistemas operativos, cambio promovido para un uso más fácil que en las versiones anteriores.

[17] http://www.guia-ubuntu.org/index.php?title=Debian

CARACTERÍSTICAS

- Ambiente gráfico
- Secuencias más rápidas de inicio y de hibernación.
- Capacidad del sistema operativo de desconectar un dispositivo externo, de instalar nuevas aplicaciones y controladores sin necesidad de reiniciar.
- Una nueva interfaz de uso más fácil, incluyendo herramientas para el desarrollo de temas de escritorio.
- Uso de varias cuentas, lo que permite que un usuario guarde el estado actual y aplicaciones abiertos en su escritorio y permita que otro usuario abra una sesión sin perder esa información.
- ClearType, diseñado para mejorar legibilidad del texto encendido en pantallas de cristal líquido (LCD) y monitores similares.

Escritorio Remoto, que permite a los usuarios abrir una sesión con una computadora que funciona con Windows XP a través de una red o Internet, teniendo acceso a sus usos, archivos, impresoras, y dispositivos;

- Soporte para la mayoría de módems ADSL y conexiones wireless, así como el establecimiento de una red FireWire.

3.2.2.3 GNU/LINUX

Sistema operativo que posee un núcleo del mismo nombre. El código fuente es abierto, por lo tanto, está disponible para que cualquier persona pueda estudiarlo, usarlo, modificarlo y redistribuirlo.

El término Linux se utiliza para describir al sistema operativo tipo Unix que utiliza filosofías y metodologías libres, y que están constituidos por la combinación del núcleo Linux con las bibliotecas y herramientas del proyecto GNU, además de otros proyectos libres y no libres.[18]

[18] http://www.alegsa.com.ar/Dic/linux.php

El término Linux también hace referencia al kernel que utilizan múltiples sistemas operativos.

CARACTERÍSTICAS

- El entorno básico del sistema operativo GNU/Linux es la línea de comando, que se ejecuta en una terminal virtual. GNU/Linux permite ejecutar hasta siete terminales virtuales, que pueden ser comandadas por usuarios distintos.
- Se distribuye su código fuente, lo cual permite a cualquier persona que así lo desee hacer todos los cambios necesarios para resolver problemas que se puedan presentar, así como también agregar funcionalidad. El único requisito que esto conlleva es poner los cambios realizados a disposición del público, esto debido a su licencia.[18]
- Es desarrollado en forma abierta por cientos de usuarios distribuidos por todo el mundo, los cuales la red Internet como medio de comunicación y colaboración. Esto permite un rápido y eficiente ciclo de desarrollo.
- Cuenta con un amplio y robusto soporte para comunicaciones y redes, lo cual hace que sea una opción atractiva tanto para empresas como para usuarios individuales.
- Linux y sus Shells: Cada usuario de un sistema Linux tiene su propia interfaz de usuario o Shell. Los usuarios pueden personalizar sus shells adecuándolos a sus propias necesidades específicas. En este sentido, el Shell de un usuario funciona más como un entorno operativo que el usuario puede controlar.
- Linux es Multitarea: La multitarea no consiste en hacer que el procesador realice más de un trabajo al mismo tiempo (un solo procesador no tiene esa capacidad), lo único que realiza es presentar las tareas de forma intercalada para que se ejecuten varias simultáneamente. Por lo tanto en Linux es posible ejecutar varios programas a la vez sin necesidad de tener que parar la ejecución de cada aplicación.
- Linux es Multiusuario: Para que pueda desarrollar esta labor (de compartir los recursos de un ordenador) es necesario un sistema operativo que

permita a varios usuarios acceder al mismo tiempo a través de terminales, y que distribuya los recursos disponibles entre todos. Así mismo, el sistema debería proporcionar la posibilidad de que más de un usuario pudiera trabajar con la misma versión de un mismo programa al mismo tiempo, y actualizar inmediatamente cualquier cambio que se produjese en la base de datos, quedando reflejado para todos.

- En conclusión, en el sistema multiusuario, varios usuarios pueden acceder a las aplicaciones y recursos del sistema Linux al mismo tiempo. Y, por supuesto, cada uno de ellos puede ejecutar varios programas a la vez (multitarea).
- Linux es Seguro: El concepto de seguridad en redes de computadores es siempre difícil de abordar. Un sistema puede ser seguro para un determinado tipo de actividades e inseguro para otras. Si se quiere que el sistema sea seguro, se debe administrar de tal forma que se tengan controlados a los usuarios en todo momento. Para la ardua tarea de seguridad surgen nuevas herramientas constantemente, tanto para detectar intrusos como para encontrar fallos en el sistema y evitar así ataques desde el exterior.
- Linux y las Redes de computadores: Cuando se trabaja con Linux se está ante un sistema operativo orientado al trabajo de redes de ordenadores.

3.2.2.3.1 Tipos de Plataformas

- Arch Linux, una distribución basada en el principio KISS con un sistema de desarrollo contínuo entre cada versión (no es necesario volver a instalar todo el sistema para actualizarlo).
- Centos, una distribución creada a partir del mismo código del sistema Red Hat pero mantenida por una comunidad de desarrolladores voluntarios.
- Debian, una distribución mantenida por una red de desarrolladores voluntarios con un gran compromiso por los principios del software libre.
- Fedora, una distribución lanzada por Red Hat para la comunidad.

- Gentoo, una distribución orientada a usuarios avanzados, conocida por la similitud en su sistema de paquetes con el FreeBSD Ports, un sistema que automatiza la compilación de aplicaciones desde su código fuente.
- GOS, una distribución basada en Ubuntu para netbooks.
- Knoppix, la primera distribución live en correr completamente desde un medio extraíble. Está basada en Debian.
- Kubuntu, la versión en KDE de Ubuntu.
- Linux Mint, una popular distribución derivada de Ubuntu.
- Mandriva, mantenida por la compañía francesa del mismo nombre, es un sistema popular en Francia y Brasil. Está basada en Red Hat.
- openSUSE, originalmente basada en Slackware es patrocinada actualmente por la compañía Novell.
- PCLinuxOS, derivada de Mandriva, paso de ser un pequeño proyecto a una popular distribución con una gran comunidad de desarrolladores.
- Puppy Linux, versión para pc's antiguas o con pocos recursos que pesa 130 mb.
- Red Hat Enterprise Linux, derivada de Fedora, es mantenida y soportada comercialmente por Red Hat.
- Ubuntu, una popular distribución para escritorio basada en Debian y mantenida por Canonical.
- Dragora y Trisquel GNU/Linux, que van adquiriendo importancia entre las distribuciones que sólo contienen software libre.
- Canaima (distribución Linux), es un proyecto socio-tecnológico abierto, construido de forma colaborativa, desarrollado en Venezuela basado en la Debian.

3.2.3 TABLA COMPARATIVA

En la siguiente tabla, se detalla las características de los sistemas operativos que se usarán para el desarrollo del proyecto.

Windows XP Professional	
Desarrollador	Microsoft Corporation
Familia de S.O	Windows
Modelo de Desarrollo	Software con licencia
Núcleo	Cerrado
Licencia	Por usuario o estación de trabajo

Tabla 3.3 Características

Fuente: Autor de la tesis

GNU/LINUX	
Desarrollador	Proyecto GNU
Familia de S.O	GNU/LINUX
Modelo desarrollo	Software Libre
Núcleo	Linux
Tipo de núcleo	Monolítico
Licencia	GLP

Tabla 3.4 Características Linux

Fuente: Autor de la tesis

Windows XP y GNU/Linux son plataformas usadas para varios requerimientos de empresas, la diferencia entre ellos es el costo, la seguridad, y la facilidad de manejo, ya que Linux no es muy amigable para los usuarios sin conocimiento alguno.

3.4 SELECCIÓN Y DETERMINACIÓN DE LA ALTERNATIVA PARA LA VPN

Luego de revisar y analizar los diferentes Software y productos de las VPN existentes en el mercado, se toma la decisión de una implementación de VPN por software.

Para la implementación de la VPN por software se toma como plataforma base para el servidor al Sistema Operativo GNU/LINUX y la distribución Debian, el software para realizar la conexión de la VPN y crear el túnel será OpenVPN.

CAPITULO 4

DISEÑO E IMPLEMENTACIÓN

En este capítulo, se revisará paso a paso las respectivas instalaciones y configuraciones de cada uno de los requerimientos que se utilizará para la conexión de la Red Privada Virtual con Debian, la configuración del open VPN para cliente y para el servidor bajo la plataforma Linux.

4.1 DISEÑO, IMPLEMENTACIÓN DE LA VPN

Una vez que se realizó el análisis de requerimientos, es necesario tener en cuenta varios aspectos importantes e identificar los elementos activos y elementos pasivos de la red para la implementación de la VPN.

4.1.1 REQUERIMIENTOS DE LA VPN

Con el estudio realizado en las oficinas de Caminosca S.A, en lo que se refiere al hardware, se revisó que los servidores que actualmente están disponibles tienen las características necesarias para la implementación de la Red Privada Virtual.

En la Empresa Caminosca, actualmente durante la transferencia de información, no se cuenta con las seguridades necesarias que garanticen la fiabilidad y seguridad en el manejo de la información.

Para garantizar las seguridades requeridas para el manejo y transferencia de información, es importante revisar las estrategias de seguridad, se recomienda revisar algunas tareas a medida que se crea el plan de seguridad de la red.

- Determinar el tipo de información que va a ser almacenada en los servidores.
- Identificar los grupos de usuarios y las necesidades de cada uno.
- Evaluar los riesgos de la seguridad e la red.
- Crear políticas de seguridad.

- Con la implementación de la Red Privada Virtual, la seguridad de la información es posible, ya que este tipo de tecnologías está basado en algoritmos de cifrado que garantizan la seguridad y la integridad de los datos.

Se deben tomar en cuenta aspectos importantes con el uso de la tecnología de Red Privada Virtual.

- Se debe designar a usuarios autorizados para el acceso a las aplicaciones y a los servidores, este aspecto es muy importante para acceder, se debe tener en cuenta a que servidores, aplicaciones y servicios tienen acceso los usuarios designados a los permisos.
- A los usuarios se les debe dar acceso con diferentes niveles de acceso.
- Toda la información debe permaneces intocables al ciento por ciento.

4.1.2 FUNCIONES DE SEGURIDAD

Se debe tener en cuenta funciones de seguridad para los sistemas operacionales, cuando se planea diseñar un sistema de seguridad para redes computacionales, algunos aspectos a tomar en cuenta son:

- **Identificación y autentificación.-** permite prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

  Se puede usar claves, tarjetas magnéticas, huellas digitales, de voz, etc. Para la identificación de los usuarios, para poder filtrar y revisar la autorización.

- **Controlar el acceso.-** Se debe evitar que algunos de los usuarios autorizados accedan a la información que no deban disponer.
- **Responsabilidad.-** asumir la responsabilidad sobre dichos recursos, a cada uno de los usuarios, es decir, cada uno debe velar por controlarlo y mantenerlo en buen estado.
- **Confiabilidad.-** Permitir que los recursos estén seguros en manos de varios usuarios.

- **Seguro.-** Proteger contra errores, modificaciones sin autorización.

4.1.3 ELEMENTOS ACTIVOS

Los elementos activos de la red de comunicación son aquellos que generan o modifican señales, con componentes que tienen circuitos integrados.[19]

Para el diseño de la Red Privada Virtual se han tomado en cuenta algunos elementos activos:

- Servidores
- Estaciones de trabajo
- Switches
- Hubs
- Modem
- Router

4.1.4 ELEMENTOS PASIVOS

Los elementos pasivos son aquellos que simplemente transmiten la información, estos no están constituidos por circuitos integrados algunos de ellos son:

- Cables
- Patch panels
- Racks
- Conectores

4.1.5 DISEÑO DE LA VPN PARA LA EMPRESA

En el siguiente gráfico, se detalla el diseño de la VPN que se utilizará para la conexión de la Vpn.

[19] http://www.alegsa.com.ar/Diccionario/C/8134.php

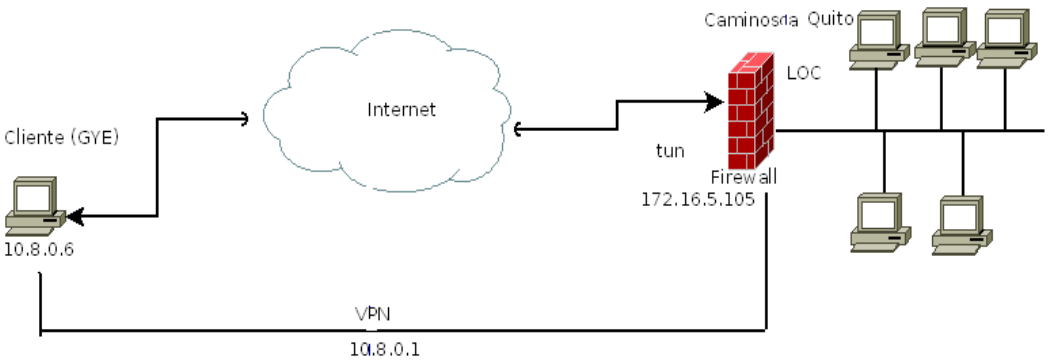

Figura 4.1 Diseño de la Vpn de la empresa

Fuente: Autor de la tesis

4.1.5.1 Funcionamiento de la VPN

Con la implementación de la Red Privada Virtual, se desea obtener las siguientes facilidades:

- Autentificación de datos y usuarios

  La VPN debe ser capaz de verificar la identidad de un usuario y restringir el acceso a la VPN de todos los usuarios que no estén autorizados. En los datos reafirmar que el mensaje a sido enviados completamente y que no ha sido alterado de ninguna forma.

- Administración de direcciones.

  Puede asignar la responsabilidad para varias direcciones IP a cada servidor, la VPN debe establecer una dirección de cliente en la red privada y cerciorarse que las direcciones se conserven así y que no sean modificadas. [20]

[20] http://www.monografias.com/trabajos11/repri/repri.shtml

- Codificación de Datos

  Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

- Administración de claves

  La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

- Soporte a protocolos múltiples

  La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet (IP), el intercambio de paquete de internet (IPX) entre otros.

4.1.6 IMPLEMENTACIÓN

Para la implementación de la Red Privada Virtual, se deben tomar en cuenta algunos aspectos que se detallan a continuación:

- La infraestructura de la red debe ser segura con el Sistema Operativo GNU/Linux, de tal manera que los equipos puedan tener comunicación entre sí.
- Verificar que los usuarios tengan una configuración del protocolo TCP/IP con una dirección IP verdadera, este paso es muy importante para la configuración de la Red Privada Virtual.
- Debe realizarse las configuraciones tanto para el servidor como para los clientes.
- Cuando la Red Privada Virtual este configurada, lo más importante es las seguridades, respecto a la información y el acceso de los clientes, la configuración de la VPN no puede ser modificada por usuarios no autorizados o intrusos que tengan acceso a la red.

- El Administrador del sistema debe poner en funcionamiento el Monitor de Red, esta permite tener datos acerca del porcentaje de utilización de la red, así como también la captura y análisis de los paquetes de red, etc.

4.1.7 INSTALACIÓN

Para la instalación de la Red Privada Virtual se tomarán en cuenta algunos aspectos:

- Se establecerá un horario para realizar las instalaciones correspondientes.
- Detallar una lista de todos los elementos que se utilizarán en la VPN.
- Verificar el servidor, si este cumple con las características recomendadas para la VPN.
- Diseñar un esquema de la red con las respectivas direcciones IP que se asignarán, todos los clientes con los cuales se hará la conexión deben tener configurado el protocolo TCP/IP que cuente con direcciones IP verdaderas.
- Tener el material adecuado para pode realizar las instalaciones.
- Realizar las configuraciones respectivas tanto para el servidor como para el cliente.

4.1.7.1 Instalación Open VPN

4.1.7.1.1 Configuración OpenVPN Servidor

Instalar OpenVPN

Como primer paso se deberá tener en cuenta que los repositorios y los programas instalados deben ser actualizados.

Se comenzará actualizando nuestro sistema con el siguiente comando.

Apt-get update

Se inicia con la instalación del software OpenVPN con el siguiente comando, el cual despliega la siguiente pantalla de instalación:

Apt-get install udev openvpn

```
Starting rpcbind daemon....

(Leyendo la base de datos ... 56979 ficheros o directorios instalados
actualmente.)

Preparando para reemplazar openssh-server 1:5.5p1-6+squeeze1 (usando
.../openssh-server_1%3a5.9p1-5_i386.deb) ...

Desempaquetando el reemplazo de openssh-server ...

Preparando para reemplazar openssh-client 1:5.5p1-6+squeeze1 (usando
.../openssh-client_1%3a5.9p1-5_i386.deb) ...

Desempaquetando el reemplazo de openssh-client ...

Selecting previously unselected package libssl1.0.0:i386.

Desempaquetando libssl1.0.0:i386 (de .../libssl1.0.0_1.0.1-4_i386.deb)
...

Preparando para reemplazar udev 164-3 (usando .../archives/udev_175-
3.1_i386.deb) ...

Desempaquetando el reemplazo de udev ...

Preparando para reemplazar libudev0 164-3 (usando .../libudev0_175-
3.1_i386.deb) ...

Desempaquetando el reemplazo de libudev0:i386 ...

Selecting previously unselected package liblzo2-2:i386.

 Desempaquetando liblzo2-2:i386 (de .../liblzo2-2_2.06-1_i386.deb) ...

Selecting previously unselected package libpkcs11-helper1:i386.

Desempaquetando libpkcs11-helper1:i386 (de .../libpkcs11-helper1_1.09-
1_i386.deb) ...

Selecting previously unselected package krb5-locales.

Desempaquetando  krb5-locales  (de  .../krb5-locales_1.10+dfsg~beta1-
2_all.deb) ...

Selecting previously unselected package openvpn.

Desempaquetando openvpn (de .../openvpn_2.2.1-8_i386.deb) ...

Procesando disparadores para man-db ...

Configurando console-setup-linux (1.75) ...
```

```
Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.ISO-8859-13.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.ISO-8859-9.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/remap.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.ISO-8859-7.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.ISO-8859-2.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.ISO-8859-4.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.ISO-8859-14.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.VISCII.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.ISO-8859-1.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.ISO-8859-15.inc ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/console-setup/compose.ISO-8859-3.inc ...

Configurando console-setup (1.75) ...

Configurando libevent-2.0-5 (2.0.18-stable-1) ...

Configurando libmount1 (2.20.1-4) ...

Configurando libwbclient0:i386 (2:3.6.3-2) ...

Configurando libkrb5support0:i386 (1.10+dfsg~beta1-2) ...

Configurando libk5crypto3:i386 (1.10+dfsg~beta1-2) ...

Configurando libkrb5-3:i386 (1.10+dfsg~beta1-2) ...

Configurando libgssapi-krb5-2:i386 (1.10+dfsg~beta1-2) ...

Configurando libtalloc2:i386 (2.0.7+git20120207-1) ...

Configurando libtdb1:i386 (1.2.9+git20120207-2) ...

Configurando libsmbclient:i386 (2:3.6.3-2) ...
```

```
Configurando nfs-common (1:1.2.5-4) ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/init.d/nfs-common ...

Replacing config file /etc/idmapd.conf with new version

Replacing config file /etc/default/nfs-common with new version

Stopping NFS common utilities: idmapd statd.

Starting NFS common utilities: statd idmapd.

Configurando rsyslog (5.8.10-1) ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/logrotate.d/rsyslog ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/logcheck/ignore.d.server/rsyslog ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/init.d/rsyslog ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/default/rsyslog ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/rsyslog.conf ...

Stopping enhanced syslogd: rsyslogd.

Starting enhanced syslogd: rsyslogd.

Configurando libssl1.0.0:i386 (1.0.1-4) ...

Configurando openssh-client (1:5.9p1-5) ...

Configurando openssh-server (1:5.9p1-5) ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/init.d/ssh ...

Restarting OpenBSD Secure Shell server: sshd.

Configurando libudev0:i386 (175-3.1) ...

Configurando udev (175-3.1) ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/init.d/udev ...

Instalando una nueva versiÃ³n del fichero de configuraciÃ³n
/etc/init.d/udev-mtab ...
```

```
Stopping the hotplug events dispatcher: udevd.

Starting the hotplug events dispatcher: udevd.

update-initramfs: deferring update (trigger activated)

Configurando liblzo2-2:i386 (2.06-1) ...

Configurando libpkcs11-helper1:i386 (1.09-1) ...

Configurando krb5-locales (1.10+dfsg~beta1-2) ...

Configurando openvpn (2.2.1-8) ...

Restarting virtual private network daemon.:.

Procesando disparadores para initramfs-tools ...

update-initramfs: Generating /boot/initrd.img-2.6.32-5-686

W: Possible missing firmware /lib/firmware/rtl_nic/rtl8105e-1.fw for
module r8169

W: Possible missing firmware /lib/firmware/rtl_nic/rtl8168e-2.fw for
module r8169

W: Possible missing firmware /lib/firmware/rtl_nic/rtl8168e-1.fw for
module r8169

W: Possible missing firmware /lib/firmware/rtl_nic/rtl8168d-2.fw for
module r8169

W: Possible missing firmware /lib/firmware/rtl_nic/rtl8168d-1.fw for
module r8169
```

Figura 4.2 Configuración de OpenVPN

Fuente: Autor de la tesis

Al instalar OpenVpn este proporciona un conjunto de herramientas están se relacionan con el cifrado llamado “easy-rsa”,estos scripts por defecto se lo encuentra en el directorio /usr/share/doc/openvpn ejemplo//easy-rsa/, los scripts que se encuentran en este directorio deben ser copiados en el directorio */etc/openvpn*

La mayor parte de la configuración para las variables de claves públicas se encuentra en este directorio *OpenVPN /etc/openvpn/easy-rsa2.0/.*

Antes de configurar las claves públicas, se debe configurar algunas variables, dentro del directorio vars, y se ejecuta el siguiente comando.

Etc/openvpn/easy-rsa/2.0/vars :/

Una vez ingresado al directorio se comprobará que el archivo vars se encuentre dentro del mismo para modificarlo posteriormente.

```
root@debian:/etc/openvpn/easy-rsa/2.0# ls

build-ca     build-key         build-key-server  clean-all  Makefile
         openssl-1.0.0.cnf           README.gz     tmp

build-dh     build-key-pass    build-req  inherit-inter    openssl-
0.9.6.cnf  openssl-1.0.0.cnf-old-copy  revoke-full  vars

build-inter  build-key-pkcs12  build-req-pass    list-crl   openssl-
0.9.8.cnf  pkitool                  sign-req     whichopensslcnf
```

Figura 4.3 Ubicación del archivo Vars

Fuente: Autor de la tesis

Para crear los certificados, es importante que la información sea precisa en especial KEY_ORG y KEY_EMAIL

```
root@debian:/etc/openvpn/easy-rsa/2.0# ./clean-all

root@debian:/etc/openvpn/easy-rsa/2.0# ./build-ca

Generating a 1024 bit RSA private key

..............++++++

.................................................++++++

writing new private key to 'ca.key'

-----

You  are  about  to  be  asked  to  enter  information  that  will  be
incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or
a DN.
```

```
There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [EC]:12

State or Province Name (full name) [PCH]:13

Locality Name (eg, city) [Quito]:14

Organization Name (eg, company) [Caminosca]:caminosca

Organizational Unit Name (eg, section) [changeme]:caminosca

Common Name (eg, your name or your server's hostname)
[changeme]:caminosca

Name [changeme]:deysi

Email Address [mail@host.domain]:deisy.cansino@caminosca^C
```

Figura 4.4 Creación de los certificados

Fuente: Autor de la tesis

Ahora se creará los certificados y clave privada para el servidor.

Dentro del directorio /etc/openvpn/easy-rsa/2.0, ejecutamos el siguiente comando:

./build-key-server "nombre de su servidor"

```
root@debian:/etc/openvpn/easy-rsa/2.0# ./build-key-server vpndeisy

Generating a 1024 bit RSA private key

......++++++

.................................++++++

writing new private key to 'vpndeisy.key'

-----

You are about to be asked to enter information that will be
```

```
incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or
a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [EC]:EC

State or Province Name (full name) [PCH]:PCH

Locality Name (eg, city) [Quito]:Quito

Organization Name (eg, company) [Caminosca]:Caminosca

Organizational Unit Name (eg, section) [changeme]:Sistemas

Common Name (eg, your name or your server's hostname)
[vpndeisy]:vpndeisy

Name [changeme]:vpndeisy

Email Address [mail@host.domain]:deisy.cansino@caminosca-sa.com



Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:tesis

An optional company name []:caminosca

Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-0.9.8.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName           :PRINTABLE:'EC'

stateOrProvinceName   :PRINTABLE:'PCH'
```

```
localityName            :PRINTABLE:'Quito'

organizationName        :PRINTABLE:'Caminosca'

organizationalUnitName:PRINTABLE:'Sistemas'

commonName              :PRINTABLE:'vpndeisy'

name                    :PRINTABLE:'vpndeisy'

emailAddress            :IA5STRING:'deisy.cansino@caminosca-sa.com'

Certificate is to be certified until Apr  7 22:31:10 2022 GMT (3650
days)

Sign the certificate? [y/n]:y
```

Figura 4.5 Creación certificados para el servidor

Fuente: Autor de la tesis

4.1.7.1.2 Implementación del Cliente

Para este objetivo, se modificará los datos y así se generan certificados y claves privadas, para cada uno de los clientes, como se muestra en la siguiente figura.

```
You are about to be asked to enter information that will be
incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or
a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [EC]:EC

State or Province Name (full name) [PCH]:PCH
```

```
Locality Name (eg, city) [Quito]:Quito

Organization Name (eg, company) [Caminosca]:Caminosca

Organizational Unit Name (eg, section) [changeme]:Sistemas

Common Name (eg, your name or your server's hostname)
[cliente1]:Guayaquil

Name [changeme]:Costa

Email Address [mail@host.domain]:guayaquil@caminosca.com


Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:guayaquil

An optional company name []:Caminosca

Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-0.9.8.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName           :PRINTABLE:'EC'

stateOrProvinceName   :PRINTABLE:'PCH'

localityName          :PRINTABLE:'Quito'

organizationName      :PRINTABLE:'Caminosca'

organizationalUnitName:PRINTABLE:'Sistemas'

commonName            :PRINTABLE:'Guayaquil'

name                  :PRINTABLE:'Costa'

emailAddress          :IA5STRING:'guayaquil@caminosca.com'

Certificate is to be certified until Apr  7 22:37:02 2022 GMT (3650
days)

Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated
```

Figura 4.6 Creación de los certificados para el cliente

Fuente: Autor de la tesis

Una vez generadas las claves privadas, se creará certificados para todos los clientes de la VPN y eso se hará con el siguiente comando:

./etc/openvpn/easy-rsa/2.0/build-key cliente1

Con este comando se crea un parámetro para cada cliente, y se crea una clave única para cada usuario de la VPN.

Se debe generar los parámetros de “Diffie Hellman” este es un método para autentificación de las claves utilizado por el servidor OpenVPN. Se ejecuta el siguiente comando para generar los siguientes parámetros:

./etc/openvpn/easy-rsa/2.0/build-dh

```
root@debian:/etc/openvpn/easy-rsa/2.0# ./build-dh

Generating DH parameters, 1024 bit long safe prime, generator 2

This is going to take a long time

....+.......+.................................+........+......+.....
.....

.............................................................+.....
.....

.....................................+.............................
.....

.............................+.....................+...............
.....

..+.............................................................+
```

```
.....

.........................+..............................++*++*++*

root@debian:/etc/openvpn/easy-rsa/2.0#
```

Figura 4.7 Generar parámetros de “Diffie Hellman”

Fuente: Autor de la tesis

A continuación se ejecuta el comando */openvpn start*, y se levanta el servicio Open vpn como se muestra en la siguiente figura.

```
root@debian:~# /etc/init.d/openvpn start
Starting virtual private network daemon: server.
root@debian:~#
```

Figura 4.8 conexión de openvpn

Fuente: Autor de la tesis

En el archivo que se creó del siguiente directorio *usr/share/doc/openvpn/examples/simple-config*, se encuentra el archivo Client.conf, este se copia en el directorio */etc/openvpn*, aquí se verifica la IP del servidor para la conexión, y se verifica los archivos que se crea para el cliente como se ve en la siguiente figura:

```
################################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
################################################

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
```

```
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one.  On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server?  Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
debian 172.16.5.105 1194
;remote my-server-2 1194

# Choose a random host from the remote
# list for load-balancing.  Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.  Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nogroup

# Try to preserve some state across restarts.
persist-key
persist-tun

# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here.  See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets.  Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
```

```
# description.  It's best to use
# a separate .crt/.key file pair
# for each client.  A single ca
# file can be used for all clients.
ca ca.crt
cert client1.crt
key client1.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server".  This is an
# important precaution to protect against
# a potential attack discussed here:
#  http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server".  The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo

# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20
```

Figura 4.9 Ip y archivos generados para el cliente

Fuente: Autor de la tesis

En el archivo *server.conf* ubicado en */etc/openvpn* se descomentará las siguientes líneas de comando para rotear y alcanzar a la red que se requirió.

push “route 192.168.10.0 255.255.255.0”

push “route 192.168.20.0 255.255.255.0”

4.1.7.1.3 Configuración Openvpn Cliente Windows

Para la configuración de nuestros clientes, se instalará el programa Openvpn GUI que contiene todos los certificados que se crean en nuestro servidor de Linux, este programa es un aplicativo totalmente gratuito y se puede descargar de internet.

Se comenzó con la instalación del programa.

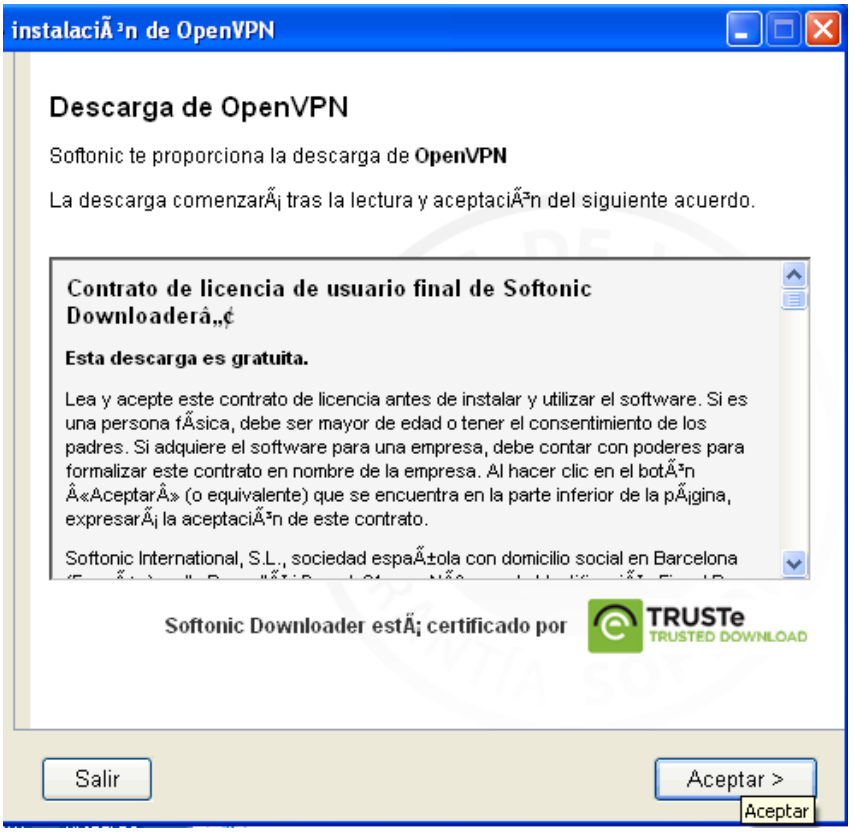

Figura 4.10 Descarga de OpenVPN Gui

Fuente: Autor de la tesis

Se acepta el contrato de licencia

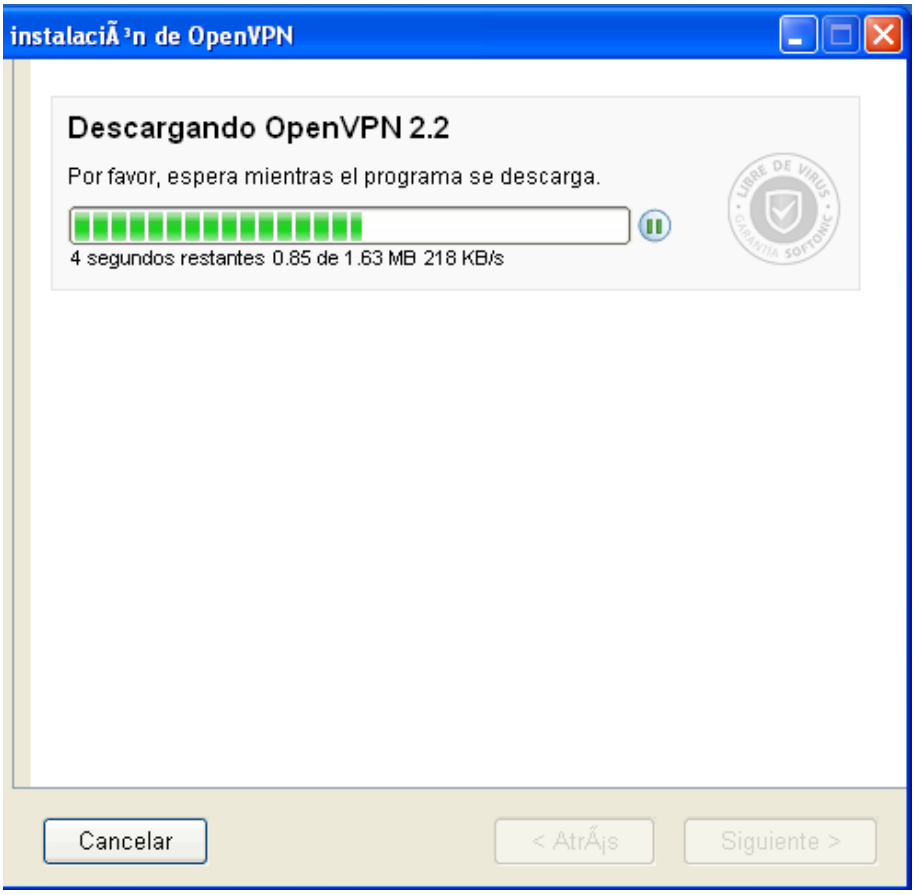

Figura 4.11 Descargando OpenVPN 2.2

Fuente: Autor de la tesis

Comienza a descargar el aplicativo bajado para la conexión entre el cliente bajo la plataforma de Windows XP con nuestro servidor Debian OPENVPN

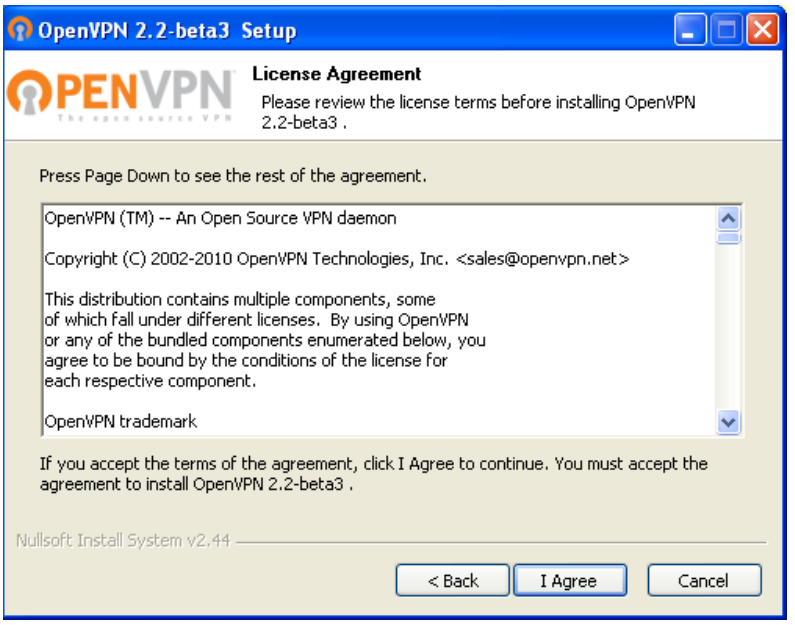

Figura 4.12 Aceptar license Agreement

Fuente: Autor de la tesis

Se acepta el contrato de licencia

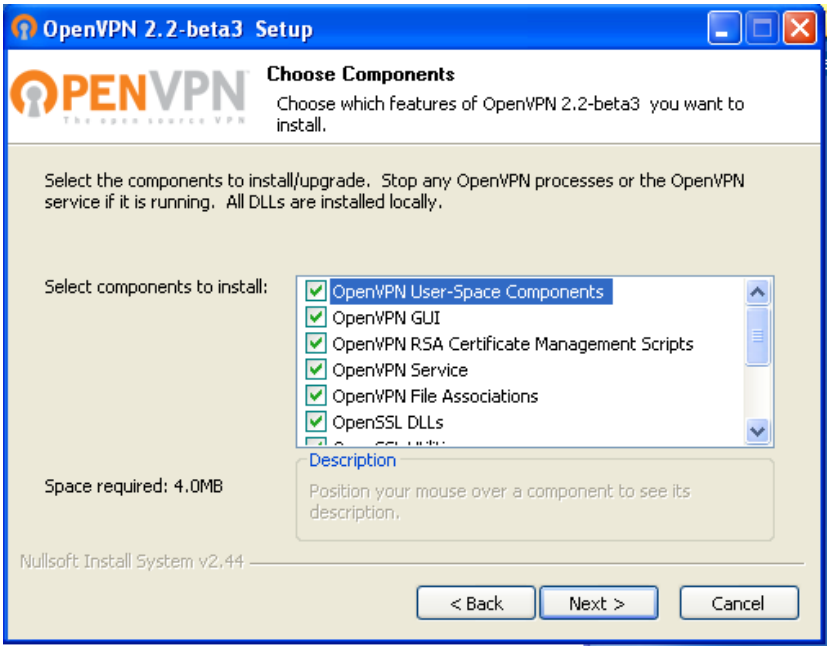

Figura 4.13 Escoger archivos a instalarse

Fuente: Autor de la tesis

Aquí se tiene la selección de componentes a instalar, se puede dejar por defecto.

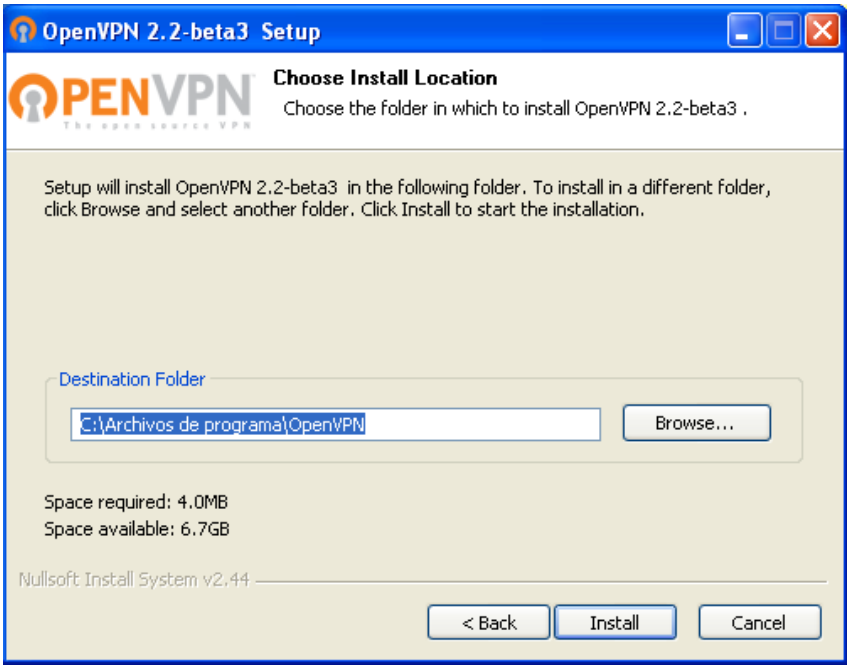

Figura 4.14 Escoger la ruta donde se descarga OpenVPN Gui

Fuente: Autor de la tesis

Se escoge la ruta donde se va a descargar el aplicativo.

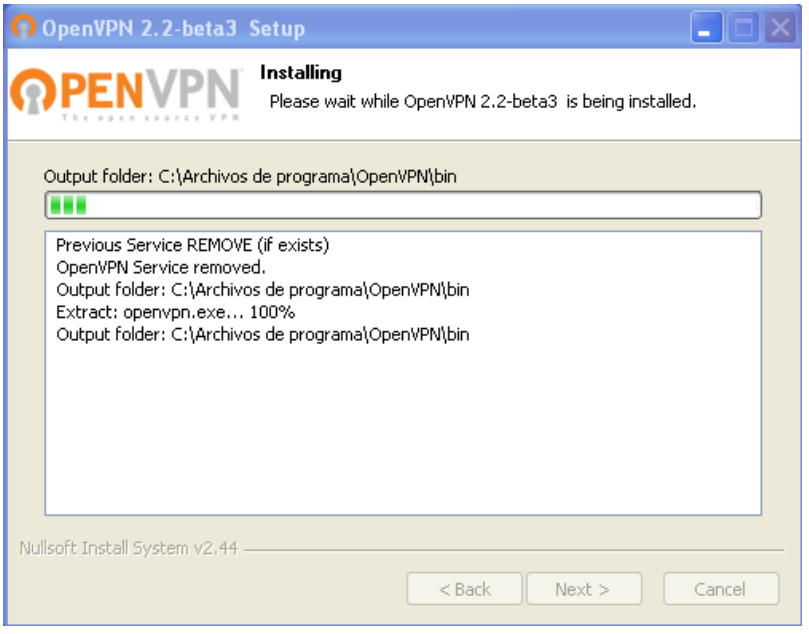

Figura 4.15 Instalación y finalización del programa

Comienza la instalación del aplicativo, y finaliza.

A continuación, se crea un icono en el escritorio del cliente del programa instalado así como se muestra en la siguiente figura.

Figura 4.16 Icono del programa

Fuente: Autor de la tesis

Con este programa, se conectará a nuestro cliente de Windows con el servidor Linux.

En el programa OpenVPN GUI dentro del directorio config se copia los siguientes ficheros que fueron creados en la instalación del servidor OpenVPN:

- ca.crt: Certificado de la autoridad certificadora
- cliente1.crt: Certificado del cliente
- cliente.key: Parte privada del certificado del cliente (clave)

Como se observa en la siguiente figura.

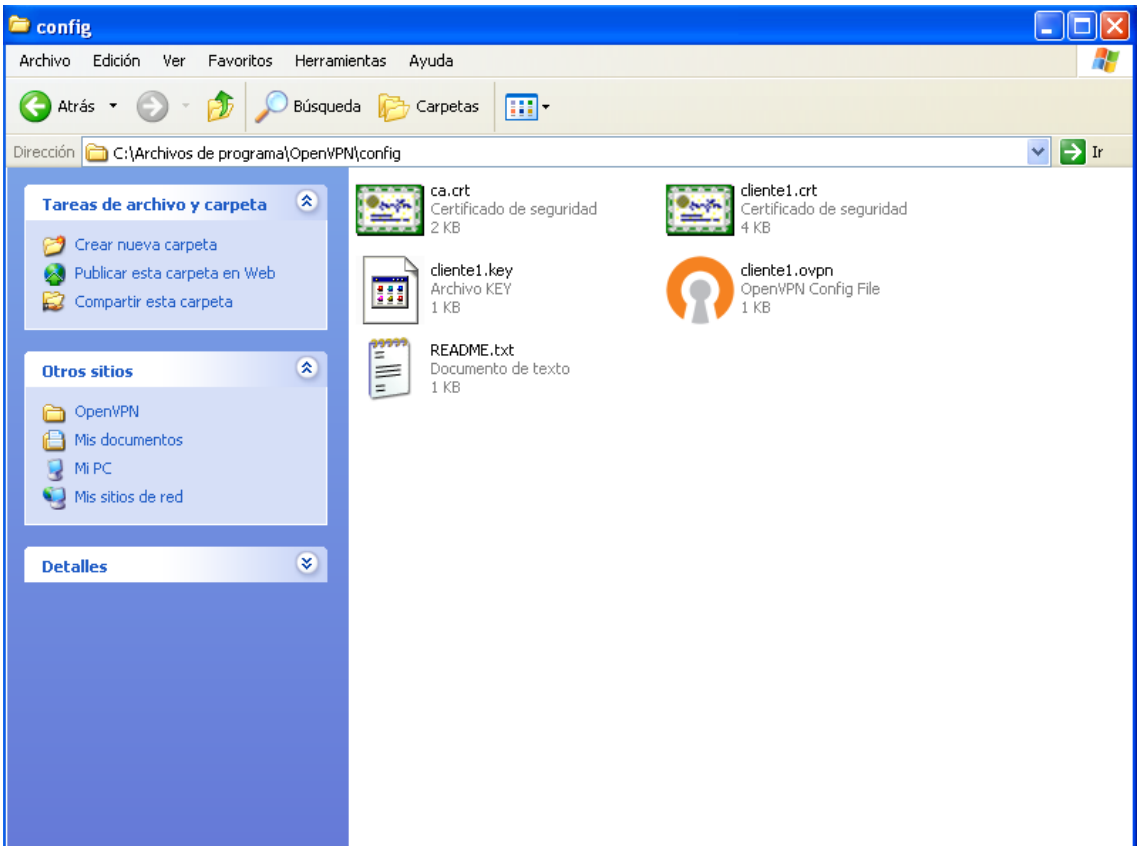

Figura 4.17 Archivos generados en Linux y copiados en el cliente

Fuente: Autor de la tesis

CAPÍTULO 5

PRUEBAS Y RESULTADOS

En este capítulo se detalla las pruebas realizadas para la conexión de la VPN, se realizó el ping necesario desde el cliente-servidor y desde el servidor al cliente para la comprobación de la conexión, se verá la transmisión de los datos, y se realizó las pruebas de tráfico las cuales se verán a continuación.

5.1 PRUEBAS DE FUNCIONAMIENTO

Primero se conectará la openvpn con el siguiente comando:

/etc/init.d/openvpn start

```
Stopping virtual prívate network daemon: server

Starting virtual private network daemon: client server
```

Figura 5.1 Inicializando Openvpn

Fuente: Autor de la tesis

Ahora en la máquina del cliente una vez inicializado el Openvpn del servidor se comprobará que estén conectados los equipos haciendo un ping a la Ip del servidor 172.16.5.105. Como se observa en la siguiente figura.

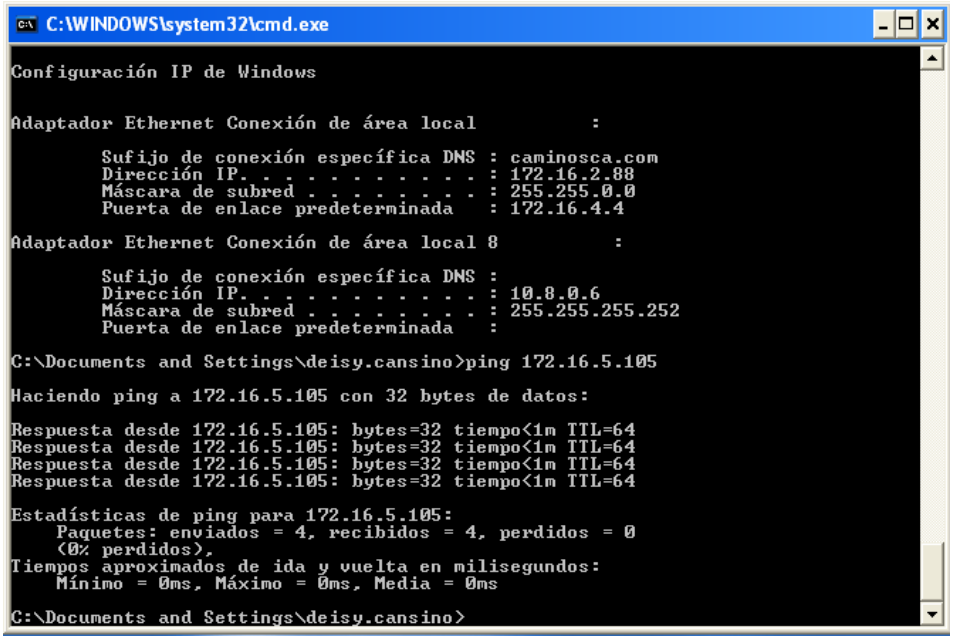

Figura 5.2 Ping conexión máquina cliente al servidor

Fuente: Autor de la tesis

Se realizó el ping desde el cliente hacia el servidor, se observa la conexión, con la respuesta que se recibe desde la Ip 172.16.5.105 que es la dirección del servidor, y se observa la dirección que se creó para el túnel 10.8.0.6.

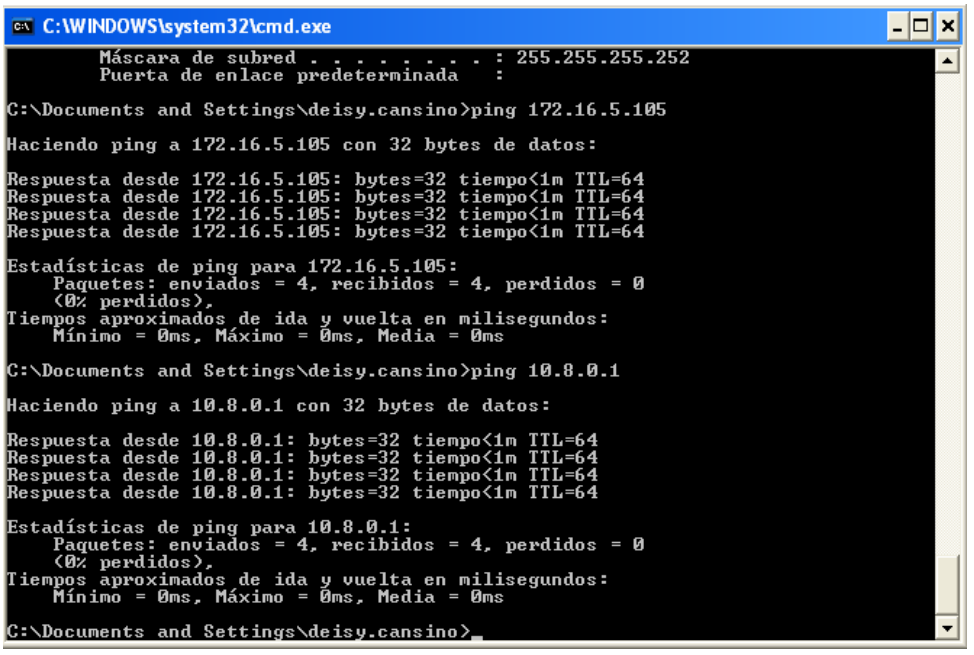

Figura 5.3 Ping conexión al túnel

Fuente: Autor de la tesis

Se realizó ping hacia la Ip del túnel, salida a internet, la Ip la genera Openvpn como seguridad. Y se observa la respuesta que se recibe al momento de hacer el ping desde la dirección del túnel, como se ve en la figura 5.4.

5.2 PRUEBAS DE CONEXIÓN

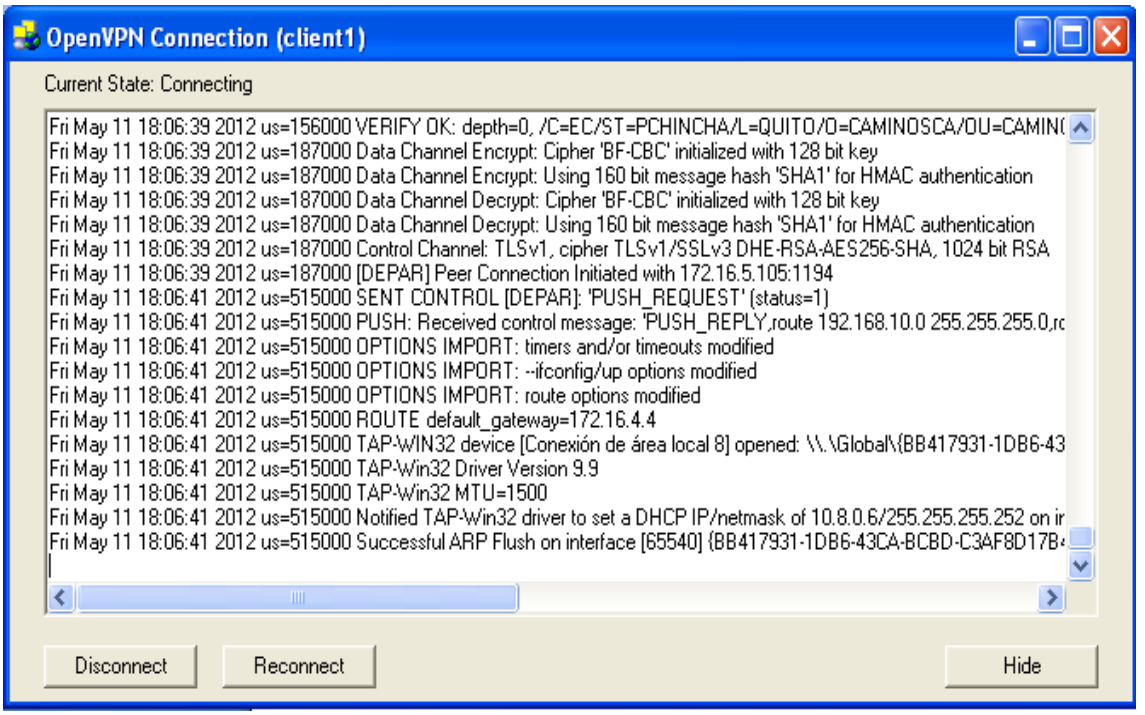

Figura 5.4 Ping conexión máquina cliente al servidor

Fuente: Autor de la tesis

En el cliente se ejecuta el programa con la conexión del Openvpn, y se realizará la conexión con el servidor OpenVPN.

Conexión del cliente con el servidor Linux

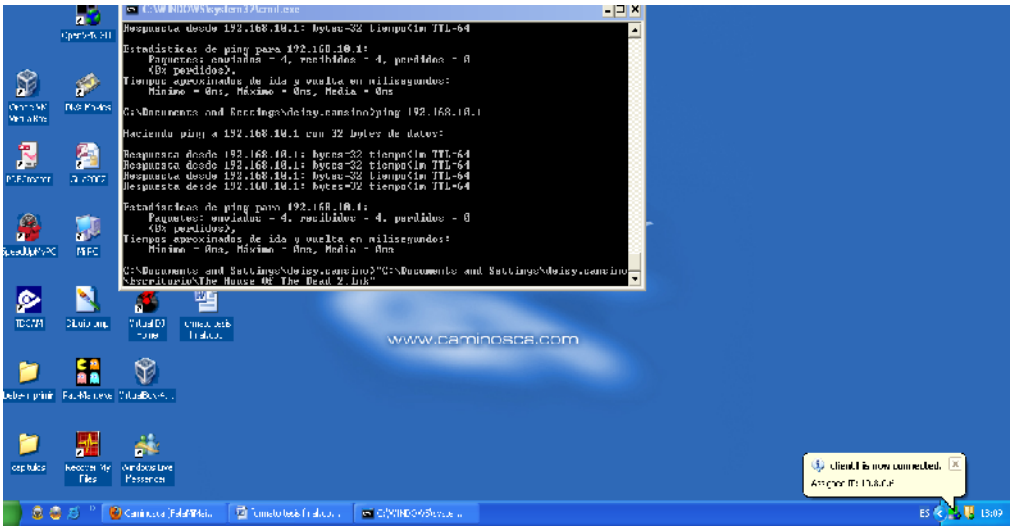

Figura 5.5 Conexión del cliente Windows con el programa OpenGui

Fuente: Autor de la tesis

Una vez conectado el programa OpenGui se genera la dirección Ip del túnel en este caso es 10.8.0.6, el icono se muestra en color verde y se tendrá la conexión establecida, como se muestra en la figura 5.6

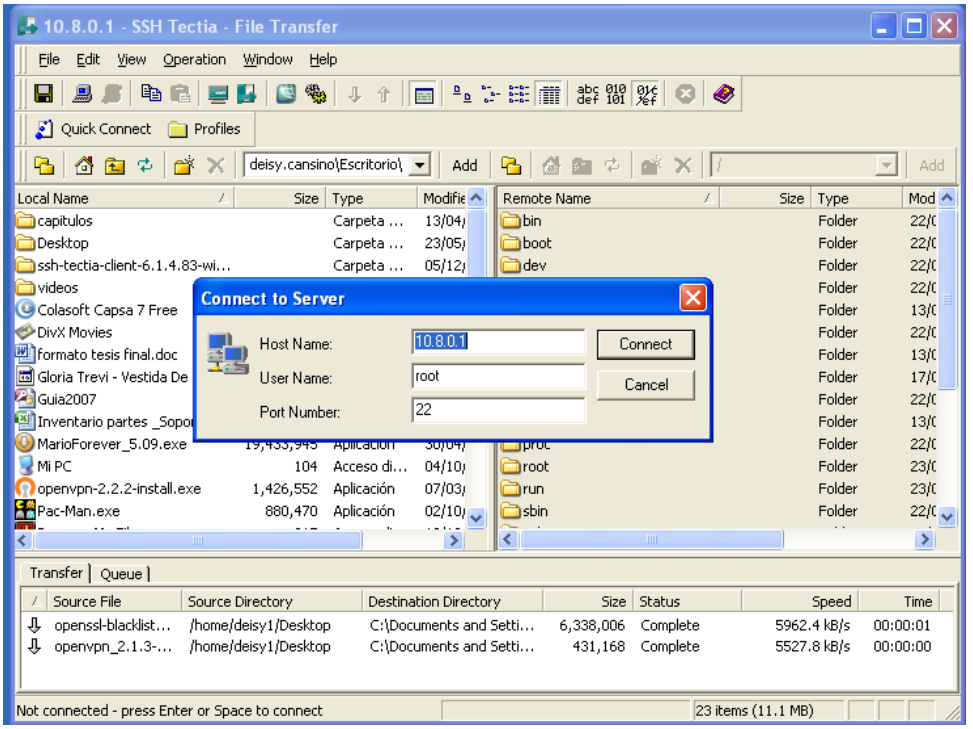

Figura 5.6 Conexión con equipo servidor

Fuente: Autor de la tesis

Se utilizará el aplicativo SSH Tectia File transfer, para la transmisión de los datos, una vez instalado se ejecuta y se ingresará la dirección del túnel, nombre del servidor, y se ingresa la contraseña.

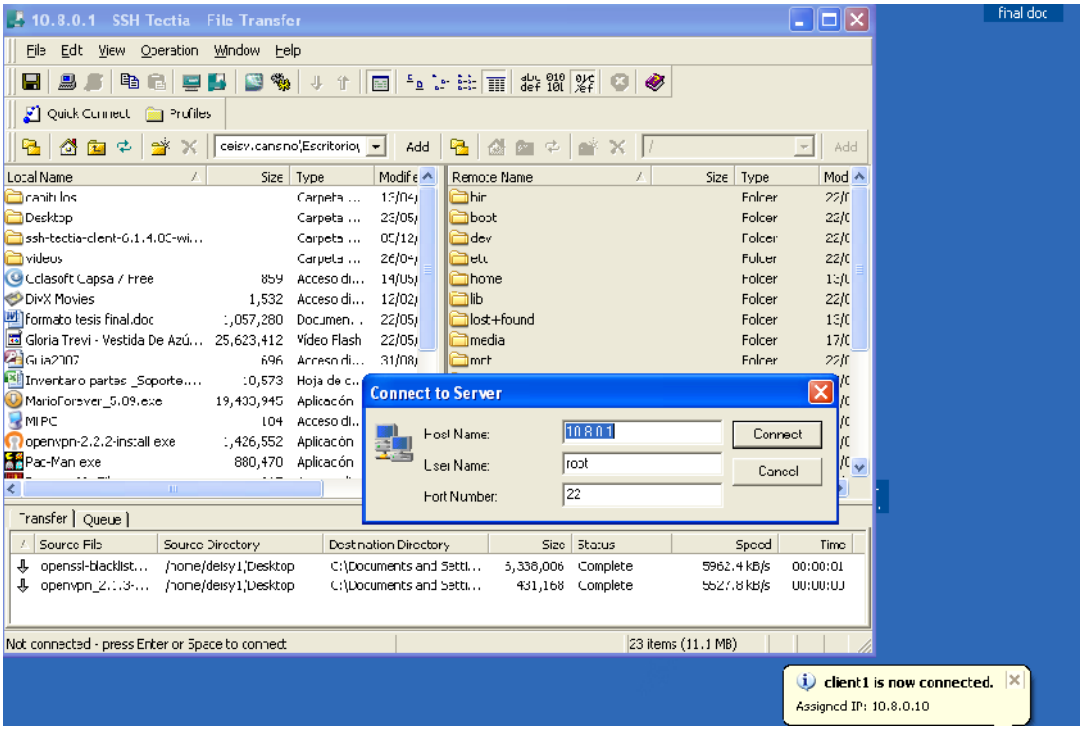

Figura 5.7 Conexión del cliente con OpenVPN

Fuente: Autor de la tesis

En este paso es verificará la conexión del cliente en el Open Vpn como se ve en la figura.

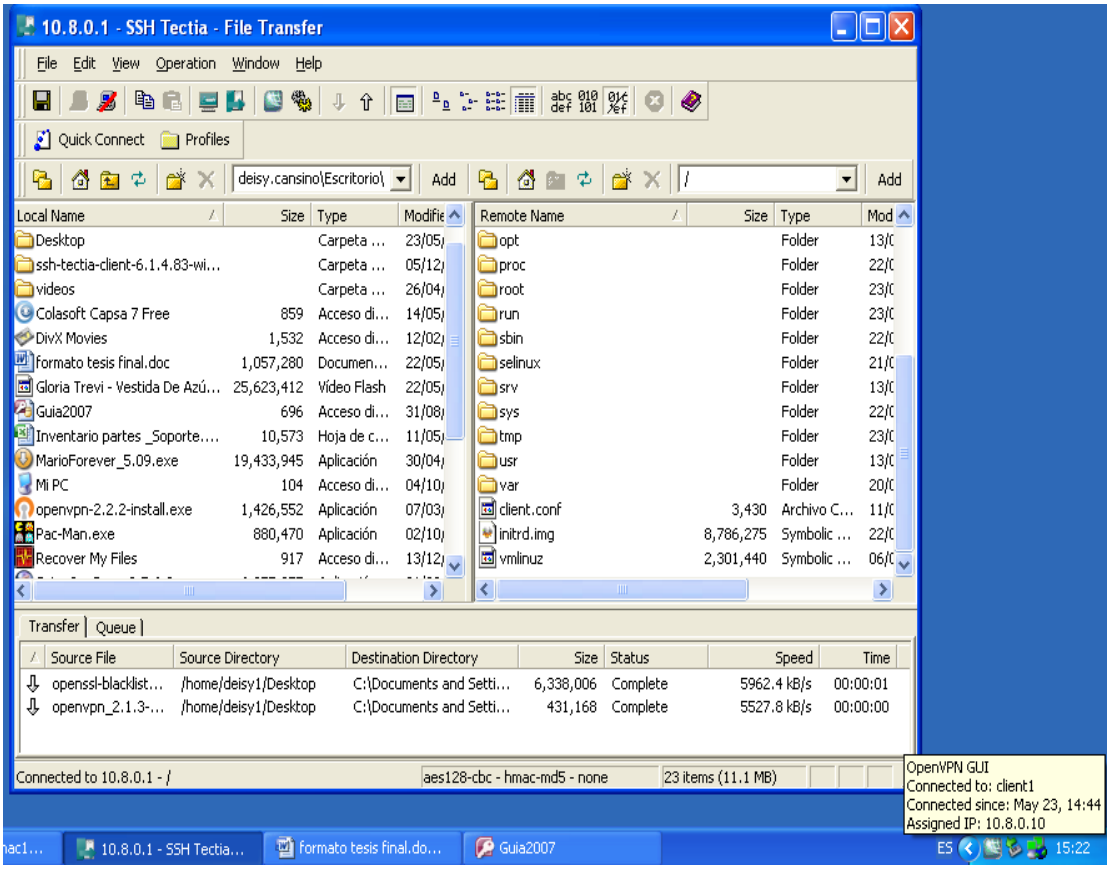

Figura 5.8 Conexión cliente y servidor

Fuente: Autor de la tesis

Se levantó el servicio SSH para la transmisión de información, en el siguiente gráfico se observa la conexión de la máquina del servidor con la máquina cliente, y la conexión del Open vpn, se puede observar las carpetas y archivos tanto del servidor (ventana 1) como del cliente (ventana 2) y así, se envía y se recibe información.

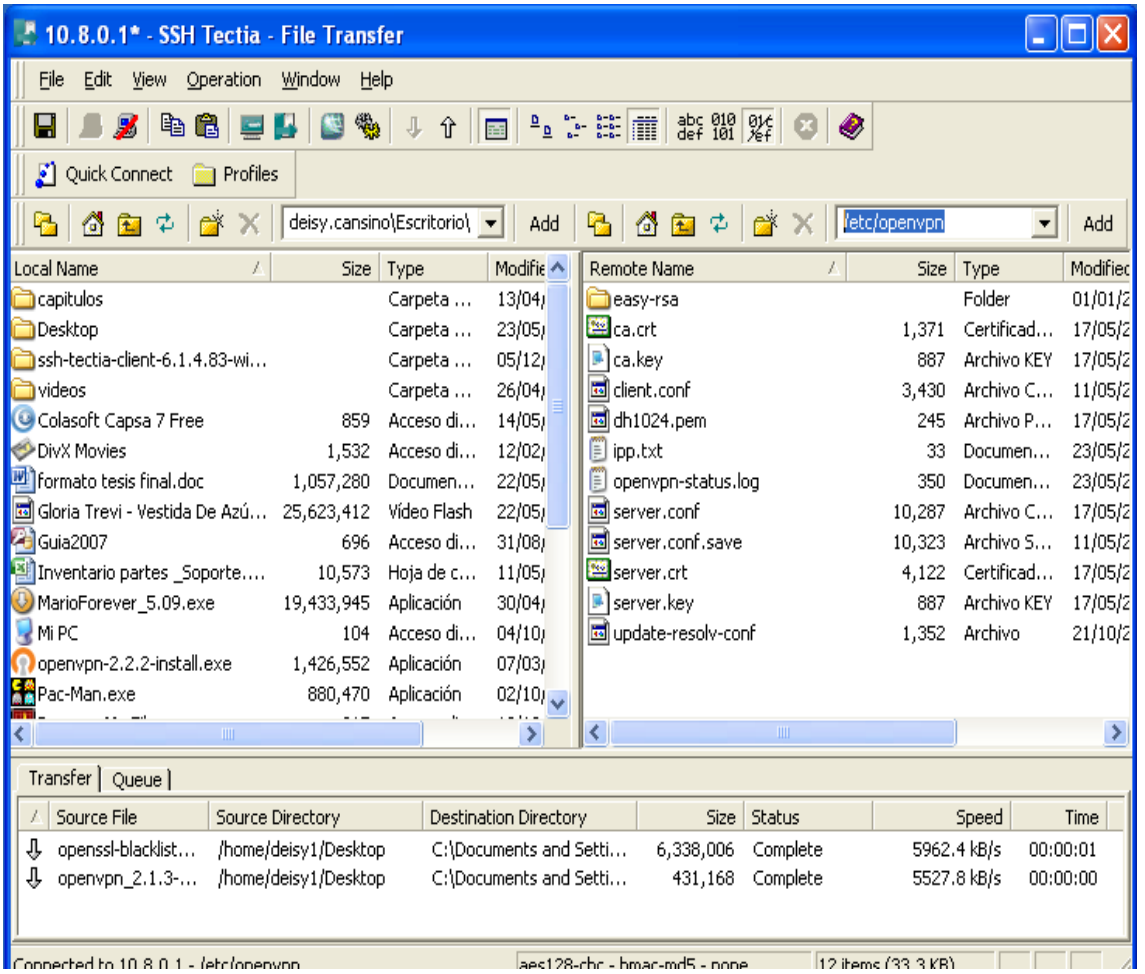

Figura 5.9 Conexión equipos

Fuente: Autor de la tesis

Se puede ingresar a las carpetas designadas para guardar la información compartirla, o enviar y recibir paquetes de datos.

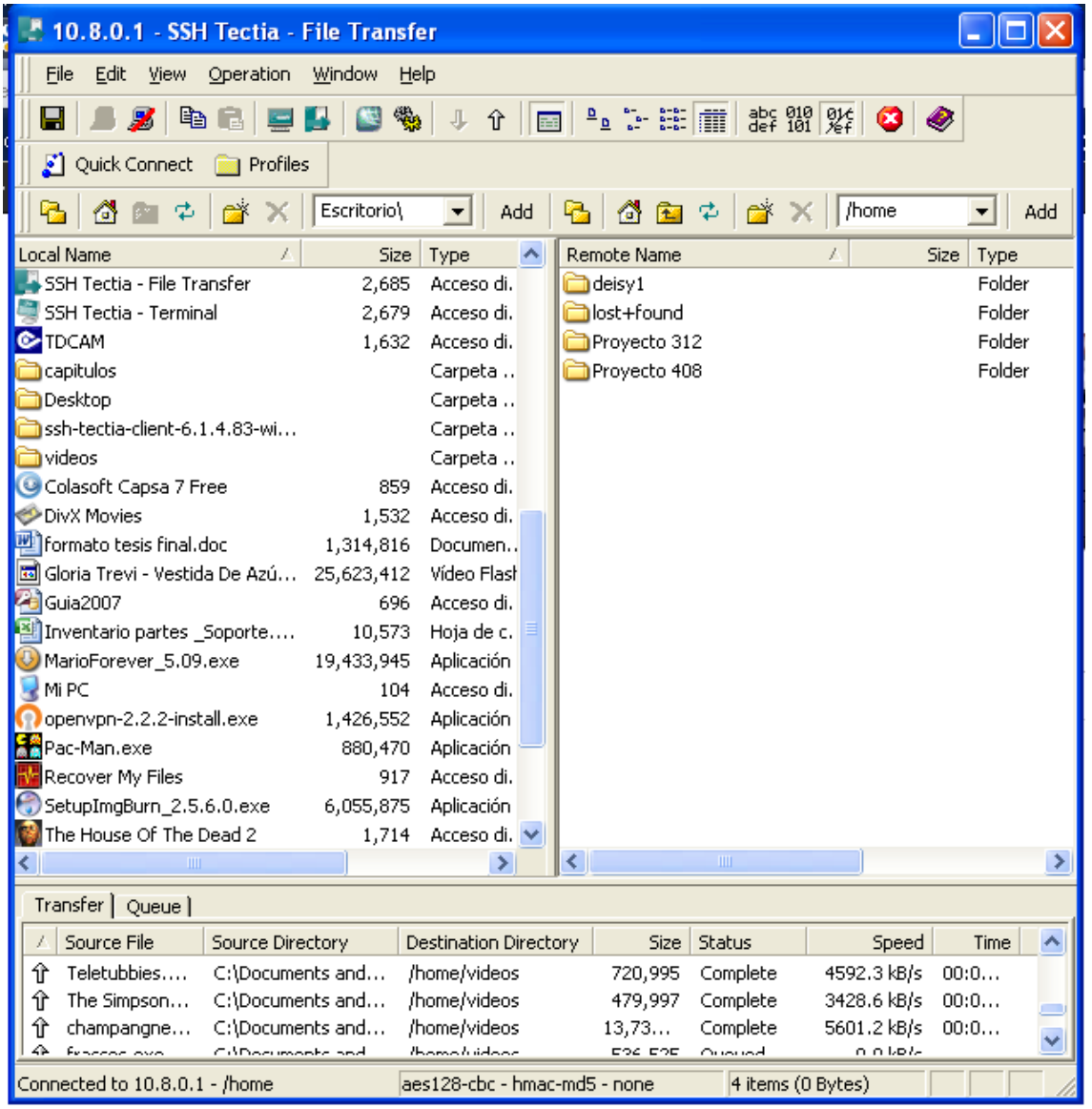

Figura 5.10 Transmisión de información

Fuente: Autor de la tesis

Se podrá copiar información tanto del servidor al cliente como del cliente al servidor, el servicio SSH detalla paso a paso la transmisión de información y como se completa la misma.

5.3 PRUEBAS DE TRÁFICO

Para realizar las pruebas de tráfico se utilizará el aplicativo Wireshark, para medir el tráfico que transmitimos desde el servidor hacia otro equipo por medio de la Vpn, ya que este nos envía la información de manera segura hacia el destino.

5.3.1 CONCEPTO

Wireshark es un capturador/analizador de paquetes de red (llamado a veces, sniffer). Wireshark analizar, aun nivel bajo y detallado, qué está pasando en tu red. Además es gratuito, open source, y multiplataforma.

Posee una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras), con este aplicativo se puede ver el tipo de tráfico que recorre la red, se puede realizar filtraciones para el tipo de protocolo que se desea observar.

5.3.2 CARACTERÍSTICAS

- Disponible para Linux y Windows
- Captura de paquetes en vivo desde una interfaz de red
- Muestra los paquetes con información detallada de los mismos
- Abre y guarda paquetes capturados
- Importar y exportar paquetes en diferentes formatos
- Filtrado de información de paquetes
- Resaltado de paquetes dependiendo el filtro

5.3.3 INSTALACIÓN Y CONFIGURACIÓN DEL APLICATIVO

Este aplicativo es gratuito se descarga y se procede con su respectiva instalación.

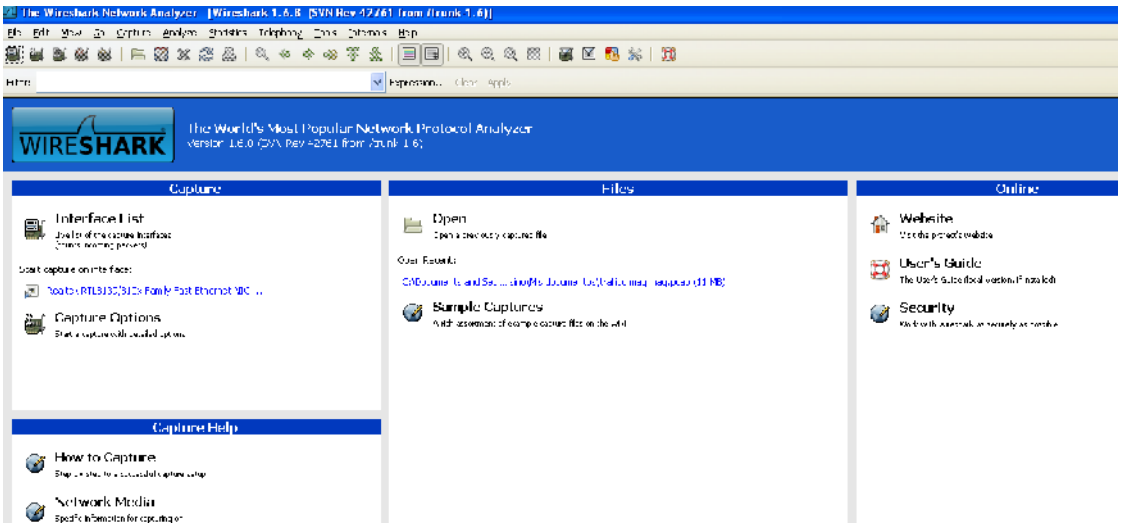

Figura 5.11 Instalación de Wireshark

Fuente: Autor de la tesis

Para la captura de información Wireshark maneja varios comandos con los que podemos trabajar, en este caso utilizaremos el comando host y la IP que permite capturar el tráfico del origen hacia el destino. Se debe especificar la interfaz de red sobre la que va a capturar los paquetes.

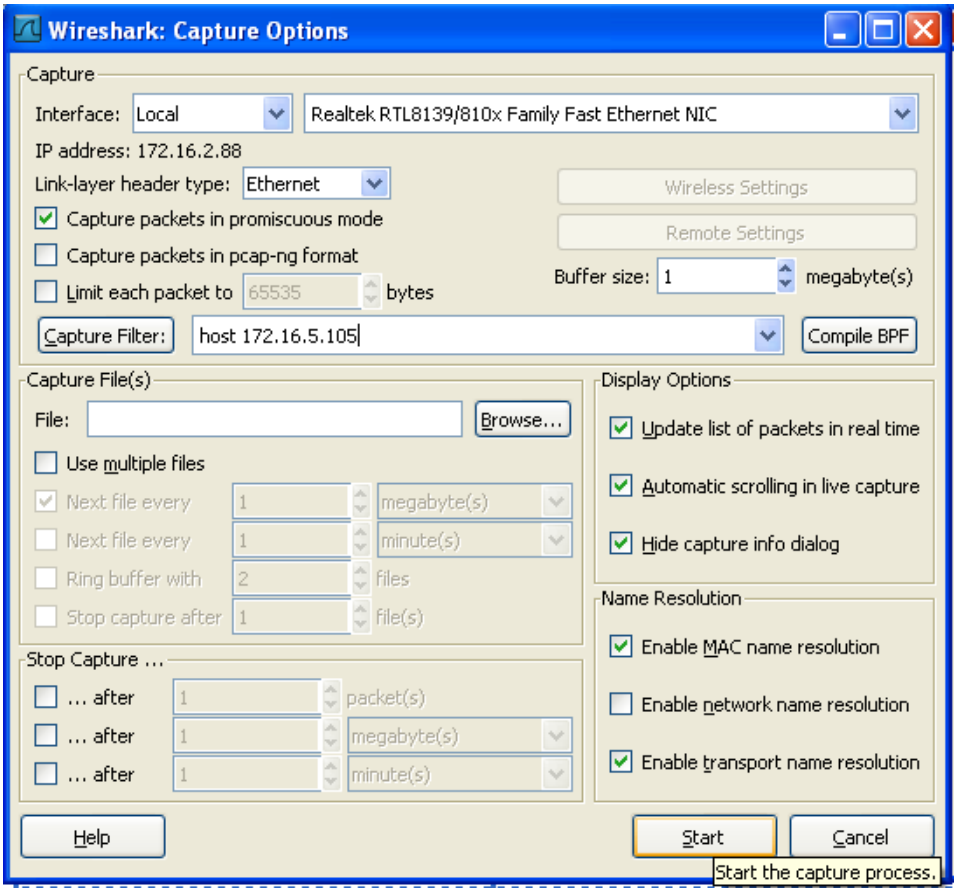

Figura 5.12 Filtros para el análisis del tráfico de la red

Fuente: Autor de la tesis

Cuando se procede a correr el aplicativo este comienza a capturar todos los movimientos de la red, en este caso enviamos un paquete de datos desde el servidor que tiene la Ip 172.16.5.105, hacia un cliente y en siguiente gráfico podemos observar como muestra un resumen de cada paquete capturado, y el tipo de protocolos que se están utilizando para la transmisión de datos.

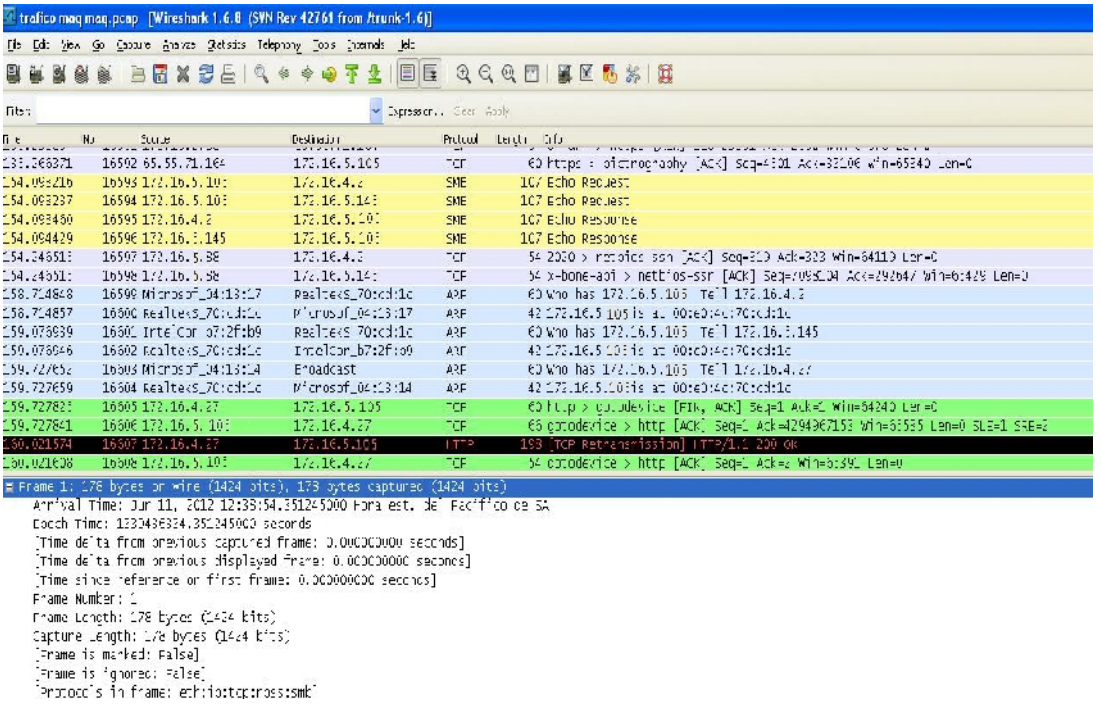

Figura 5.13 Análisis del tráfico desde el servidor al cliente

Fuente: Autor de la tesis

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Uno de los principales objetivos de este proyecto fue intercambiar información a través de una red pública entre los usuarios de la oficina matriz con los usuarios de las oficinas sucursales de la empresa Caminosca S.A., proporcionando seguridad, confiabilidad y rapidez. Esto se logró con la configuración de una VPN realizada en GNU/Linux, en el servidor ubicado en la oficina matriz de Caminosca.

- Con el uso de la Red Privada Virtual se puede determinar que son una buena opción para la comunicación entre computadores, son fiables para la transmisión de información la cual es muy importante para la empresa Caminosca S.A., ya que ha permitido desarrollar sus actividades en cada una de las áreas. Los usuarios pueden comunicarse e intercambiar información por medio de la VPN.

- Con la configuración de la Vpn se realizó la conexión de la empresa matriz con las oficinas sucursales de manera exitosa, y se cumplió con los objetivos, esto se demostró con las pruebas de conexión, envío y recepción de datos.

- Mediante la realización de este proyecto se comprobó que el uso de una Red Privada Virtual bajo la plataforma de Linux, es muy conveniente para la empresa en conceptos de costos, y este tipo de conexión nos permite tener una comunicación muy segura.

- Los usuarios que laboran en las oficinas sucursales, con la conexión de la VPN pueden hacer uso de la información de la empresa, de las oficinas matriz de manera más rápida y sin el miedo de perder o que la información pueda ser filtrada por usuarios ajenos a la empresa.

- La implementación de VPN fue factible para la empresa, ya que se logró transmitir información de manera segura y rápida, y no es necesario contratar un enlace directo, en la conexión entre el servidor y el cliente.

RECOMENDACIONES

- Se puede implementar una Red Privada Virtual en cualquier tipo de red para realizar la transferencia de información, de manera segura y confiable.

- Para el correcto funcionamiento de la Red Privada Virtual se debe tener en cuenta el tipo de equipos a usar, y el tipo de servicio de internet que provee a la empresa.

- Para obtener la información de la oficina Matriz, el administrador de la red pondrá a su disposición el tipo de seguridades y permisos para ingresar a la misma, a los usuarios de las oficinas sucursales, dependiendo del tipo de trabajo a realizarse en el mismo.

- Como recomendación final en caso de que la empresa tenga más usuarios en la conexión y la red de la empresa crezca, se debe tomar en cuenta el Servicio de Internet contratado para el correcto funcionamiento de la VPN.

BIBLIOGRAFÍA

[1] Nombre del autor: Copyright © 2012 MSM - Soluciones Informáticas Título: Redes y comunicaciones Recuperado el: 17/05/2011, de http://ondinet.net/msm/index.php?option=com_k2&view=item&layout=item&id=19&Itemid=235

[2] Título: Tipos de redes Recuperado el: 20/06/2012, de: http://mantenimientodecomputadora.webs.com/tiposderedes.htm

[3] Título: Red Privada Virtual: Recuperado: miércoles, 8 de marzo de 2011, 09:32, de:

http://campusvirtual.unex.es/cala/cala/mod/resource/view.php?id=1875

[4] Título: Textos Científicos VPN, recuperado el Vie, 03/11/2011 - 18:04, de http://www.textoscientificos.com/redes/redes-virtuales/vpn

[5] Título: Qué es y cómo crear una VPN, recuperado el: 15/10/2010, de http://www.configurarequipos.com/doc499.html

[6] Nombre del Autor: Compass,corp, Título: Protocolo, recuperado el: 14/08/2010, de:

http://www.designcompasscorp.com/index.php?option=com_categoryblock&view=article&Itemid=118&id=73

[7] Título: INTRODUCCION A LAS REDES PRIVADAS VIRTUALES (VPN) BAJO GNU/LINUX, recuperado el 25 de julio del 2012, de

http://www.lugro.org.ar/biblioteca/articulos/vpn_intro/vpn_intro.html

[8] Título: Vpn — Presentation Transcript, recuperado el 15/09/2010, de: http://www.slideshare.net/paulguachamin/vpn-7863465

[9] Autor: Javier Eduarte, Título: Usar SSH para crear un proxy HTTP, recuperado el 14/06/2011, de:

http://www.linuxparatodos.net/portal/article.php?story=sockets

[10] Autor: Ecured, Título: Protocolo TLS (Transport Layer Security, recuperado el: Sábado, 5 de mayo de 2012 de: http://www.ecured.cu/index.php/TLS

[11] Autor: Created by Pablo Gonzalez and Juan Antonio Calles Copyright © 2012 Flu Project info@flu-project.com**,** Título: Configuración Servidor SSH en GNU/Linux, recuperado el 2012 de: http://www.flu-project.com/configuracion-servidor-ssh-en-gnulinux.html

[12] Autor: Crolina Quinodóz, Título: Cómo crear una red VPN, recuperado el: 2012, de: http://profecarolinaquinodoz.com/principal/?tag=concepto-de-red-vpn

[13] Autor, Fernando de la cuadra, Título: Seguridad en conexiones VPN, recuperado el 2010, de:

http://www.pandasecurity.com/NR/rdonlyres/6647F8ED-F5EA-4E73-AA5C-9B038B71F916/3176/VPN_spa_010205_2146481243.pdf

[14] Título: Introducción a la informática, recuperado el: 2011, de: http://usuarios.multimania.es/lenoel/

[15] Autor: Exal de Jesús García Carrillo, Título: Introducción a Linux, recuperado:2011, de:

http://www.monografias.com/trabajos24/linux/linux.shtml

[16] Autor: Caminosca, Título: Red que conforma la red sucursal de Caminosca, recuperado el: 2011.

[17] Título: Debian, recuperado el: 2011, de: http://www.guia-ubuntu.org/index.php?title=Debian

[18] Título: definición de Linux, recuperado el: 2012 de:

http://www.alegsa.com.ar/Dic/linux.php

[19] Título: Definición de Linux (GNU/Linux), recuperado el: 2011 de: http://www.definicionabc.com/tecnologia/linux.php

[20] Autor: Debian, Título: Acerca de Debian, recuperado el: 2012 de: http://www.debian.org/intro/

[21] Título: OpenVPN, recuperado el: 2011 de:

https://sites.google.com/a/terminuspro.com/internet/manuales/openvpn

[22] Autor: Ecualug, Título: Como instalar y configurar Openvpn recuperado el :Mar, 2007-02-06 15:52 de:

http://www.ecualug.org/2007/02/06/comos/centos/c_mo_instalar_y_configurar_openvpn

GLOSARIO

- FTP.- protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor, o apropiarse de los archivos transferidos.

Para solucionar este problema son de gran utilidad aplicaciones como scp y sftp, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.

- TUNNELING.- consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH..

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su *home-agent* realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

- ENCAPSULACIÓN.- se denomina encapsulamiento al ocultamiento del estado, es decir, de los datos miembro, de un objeto de manera que sólo se puede cambiar mediante las operaciones definidas para ese objeto.

Cada objeto está aislado del exterior, es un módulo natural, y la aplicación entera se reduce a un agregado o rompecabezas de objetos. El aislamiento protege a los datos asociados a un objeto contra su modificación por quien no tenga derecho a acceder a ellos, eliminando efectos secundarios e interacciones.

De esta forma el usuario de la clase puede obviar la implementación de los métodos y propiedades para concentrarse sólo en cómo usarlos. Por otro lado se evita que el usuario pueda cambiar su estado de maneras imprevistas e incontroladas.

- ENCRIPTACIÓN.-consiste en codificarlo para que resulte indescifrable a cualquier persona que no conozca la clave para poder descifrarlo. Por ello la encriptación es aquel proceso por el que la información es cifrada para que resulte ilegible a menos que conozcamos los medios para su interpretación.

En informática sería la codificación gracias al uso de diversas fórmulas matemáticas con el objetivo de transformar un texto o imágenes en un criptograma. Que es un conjunto de caracteres que a simple vista no tiene ningún sentido para el navegante. En la mayoría de los casos se utiliza una palabra clave para poder descifrar el mensaje que se ha cifrado con anterioridad.

Con esta clave evitamos que cualquier intruso pueda descifrar el criptograma si conoce la fórmula para descodificarlo. Porque además necesitara esta clave para poder traducir el mensaje cifrado. Por lo que en algunas ocasiones se utilizan dos claves para una mayor seguridad.

- ANCHO DE BANDA.- es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período dado. El ancho de banda se indica generalmente en bits por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps).

Para señales analógicas, el ancho de banda es la longitud, medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. Puede ser calculado a partir de una señal temporal mediante el análisis de Fourier. También son llamadas frecuencias efectivas las pertenecientes a este rango.

- CONEXIÓN REMOTA.- consiste en conectarse por la red a otro ordenador como si se accediera desde el propio ordenador. Esta conexión puede realizarse mediante la creación de redes privadas virtuales, por ejemplo, en una empresa o una Universidad, para que cualquier usuario pueda acceder a la información que desee desde cualquier ordenador, siempre que tenga instalada la red de Internet. Para que no haya problemas de seguridad, cuando se crea este tipo de conexión, para obtener los datos el internauta debe tener una cuenta de usuario y contraseña propias.

- SSH.- (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar

los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

- MULTICAST.- es un servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, puede ser enviada simultáneamente para diversos destinatarios. El multicast es dirigido para aplicaciones del tipo uno-para-varios y varios-para-varios, ofreciendo ventajas principalmente en aplicaciones multimedia compartidas.

- DNS (Domain Name System).- es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.mx y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

- PROXY.- Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

- LINUX.- Linux es muy eficiente y tiene un excelente diseño. Es multitarea, multiusuario, multiplataforma y multiprocesador; en las plataformas Intel corre en modo protegido; protege la memoria para que un programa no pueda hacer caer al resto del sistema; carga sólo las partes de un programa que se usan; comparte la memoria entre programas aumentando la velocidad y disminuyendo el uso de memoria; usa un sistema de memoria virtual por páginas; utiliza toda la memoria libre para cache; permite usar bibliotecas enlazadas tanto estática como dinámicamente, se distribuye con código fuente, tiene un sistema de archivos avanzado pero puede usar los de los otros sistemas; y soporta redes tanto en TCP/IP como en otros protocolos.

- KERNEL.- El kernel ó núcleo de linux se puede definir como el corazón de este sistema operativo. Es el encargado de que el software y el hardware de tu ordenador puedan trabajar juntos.

Las funciones más importantes del mismo, aunque no las únicas, son:

- Administración de la memoria para todos los programas y procesos en ejecución.
- Administración del tiempo de procesador que los programas y procesos en ejecución utilizan.
- Es el encargado de que podamos acceder a los periféricos/elementos de nuestro ordenador de una manera cómoda.

Hasta que empezó el desarrollo de la serie 2.6 del núcleo, existieron dos tipos de versiones del núcleo:

- *Versión de producción:* La versión de producción, era la versión estable hasta el momento. Esta versión era el resultado final de las versiones de desarrollo o experimentales.

  Cuando el equipo de desarrollo del núcleo experimental, decidía que tenía un núcleo estable y con la suficiente calidad, se lanzaba una nueva versión de producción ó estable. Esta versión era la que se debía utilizar para un

uso normal del sistema, ya que eran las versiones consideradas más estables y libres de fallos en el momento de su lanzamiento.

- *Versión de desarrollo:* Esta versión era experimental y era la que utilizaban los desarrolladores para programar, comprobar y verificar nuevas características, correcciones, etc. Estos núcleos solían ser inestables y no se debían usar sin saber lo que se hacía.

- GNU.- El sistema GNU fue diseñado para ser compatible con UNIX, un sistema operativo que no es libre.

Este sistema se lanzó bajo una licencia denominada copyleft, para que cualquier usuario pueda ejecutar, copiar, modificar o distribuir el sistema. Esta licencia está contenida en la Licencia General Pública de GNU (GPL).

- UNIX.- Es una familia de sistemas operativos tanto para ordenadores personales como para mainframes. Soporta gran número de usuarios y posibilita la ejecución de distintas tareas de forma simultánea (multiusuario y multitarea). Su facilidad de adaptación a distintas plataformas y la portabilidad de las aplicaciones.

- SHELL.- Es un tipo de utilidad cuya finalidad consiste en hacer más fácil el manejo del sistema operativo o de una aplicación por parte del usuario.

Se llama shell al intérprete de comandos o programa que permite introducir órdenes en una computadora.

- IPSEC.- IPSec autentifica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre estaciones de trabajo y servidores, y entre servidores. El objetivo principal de IPSec es proporcionar protección a los paquetes IP. IPSec está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.